

G Data Business Software

User Manual



G Data. Security **Made in Germany.**

目次

G Data Business

グローバルネットワーク化とそれに伴うセキュリティリスクの増大は、企業においては、もはやIT担当者のみの問題ではありません。リスクマネジメントの観点からも、マネジメントからの視点はもちろんのこと、社内全体で考えていくべき重要なテーマです。ウイルスが引き起こす被害（ネットワークダウン、機密情報や顧客情報の情報漏洩など）は、企業経営に大打撃を与えかねない深刻な問題となっています。

G Data は、多くのテスト機関やメディアから数々の賞を受賞し、業界最高レベルのウイルス保護を提供するリーディングカンパニーです。G Data 法人版には、ユーザーの使い心地を考慮して開発され、最新の保護メカニズムが搭載された中央管理型ウイルス対策ソリューションです。あなたの社内ネットワーク内のクライアントPC、サーバー、モバイル端末を、最新のセキュリティリスクから効果的に守ります。

ウイルス対策の全プロセスは、バックグラウンドで行われるため、それぞれのクライアントPCで作業をしているユーザーを煩わすことはありません。最新の脅威へ速やかに対応できるように、ウイルスの定義ファイル更新は短間隔で配布されます。

G Data 法人版の中央管理を担う G Data ManagementServer は、インストール、設定、更新、といった遠隔管理を可能にし、システム管理者に掛かる負荷、時間やコストなどを軽減することができます。

G Data 法人製品をご愛顧頂きますよう宜しくお願い致します。

G Data Team

<u>製品アップグレード</u>

本マニュアルでは、G Data 法人製品の全機能の機能を解説しています。ご利用の製品をアップグレード（製品を切換えて機能を追加）したい場合は、G Data または販売代理店までお問い合わせください。

<u>マニュアルについて</u>

本マニュアルのスクリーンショットは、開発中もしくは英語版の画面を使用しております。そのため、実際の操作画面とはスクリーンショット内の表記が異なる場合がありますのであらかじめご了承ください。

各製品の機能

G Data 法人製品は、小規模事業者から大規模な企業環境まで、あらゆるサイズのネットワーク環境に対応できる包括的な保護を提供するため、様々な製品ラインナップを用意しています。それぞれの製品には多彩な先進技術が搭載されており、堅牢なセキュリティ・高パフォーマンスを簡単な操作で実現しています。

各製品にどの製品が対応しているかは、以下の表でご確認ください。

G Data...	AntiVirus	Firewall	AntiSpam	PolicyManager	BankGuard	Report-Manager	MobileDevice Management
AntiVirus Business	■				■	■	■
ClientSecurity Business	■	■	■		■	■	■
EndpointProtection Business	■	■	■	■	■	■	■

マニュアルに関して

G Data 製品の使用方法に関する詳細なヘルプは、F1 キーで呼び出すことができます。また、以下の G Data のサイトからPDF版のマニュアルデータをダウンロードできます。

日本: www.gdata.co.jp/support/download
USA: www.gdata-software.com
United Kingdom: www.gdatasoftware.co.uk
International: www.gdatasoftware.com

セキュリティラボ

新種の脅威や不審な現象やファイルを確認した場合、隔離から当該ファイルを G Data セキュリティラボに送信できます。

これを実行するには、まず G Data Administrator のレポート画面で感染ファイルを隔離します。次に、隔離されているファイルを右クリックし、**隔離: G Data セキュリティラボに送信** を選択します。これで G Data セキュリティラボ へのファイル送信は完了です。

送信されたファイルは、すぐに G Data セキュリティラボにて検証分析し、対策を提供します。提出されたファイルは、ドイツ連邦共和国の個人情報保護法に基づき、G Data によって細心の注意を払い取り扱われます。

G Data セキュリティラボの返信送付先メールアドレスは、G Data Administrator の **オプション** > **サーバー設定** > **メール設定** から設定できます。

サポート

操作方法など、ご購入後の製品に関するお問い合わせは、ユーザーサポートで受付いたします。
※体験版の場合は、ユーザーサポートのご利用はできません。予めご了承ください。

ユーザーサポートの連絡先

問い合わせ先については、製品購入時の資料をご確認ください。

1. サポート期間

ライセンス有効期間内

2. サポート範囲

製品のご利用の説明、疑問点にお答えするサービスとさせていただきます。
以下の場合には、お問い合わせに対してのご回答ができませんので、予めご了承ください。

a) 本製品で保証している動作環境外でのお問い合わせ
b) 本製品ではないもの（ハードウェア・他社製品）に関するお問い合わせ
c) サポート時間外のサポートおよび、指定された方法以外の方法でのサポートのご依頼

3. ユーザーサポートをお受けになる際に

お問い合わせの際は、お客様番号または、レジストレーション番号をご用意いただき、更に質問要点を整理していただいた上で、お問い合わせいただきますようお願いいたします。

インストール

Windows を起動し、本製品の製品メディアをドライブにセットしてください。自動的にインストール画面が表示されます。インストール開始前は、他のプログラムを終了していることを確かめてから実行してください。［**インストール**］ボタンを押すと、以下のインストールするモジュールの選択画面が表示されます。



- **G Data ManagementServer**: G Data 法人製品を初めてインストールする場合は、まずこのコンポーネントをインストールします。G Data ManagementServer は、G Data 法人版製品の各種設定や更新を管理するためのコアインスタンスです。G Data ManagementServer をインストールすると、G Data Administrator も自動的にインストールされます。

- **G Data Administrator**: G Data Administrator は、G Data ManagementServer の管理コンソールです。ネットワーク内の G Data インストール済みクライアントの設定や更新を一元管理できます。G Data Administrator にはパスワード保護が掛けられ、G Data ManagementServer と接続されている Windows PC へインストールしたり、起動ができます。
- **G Data Security Client**: G Data Security Client は、G Data ManagementServer からのタスクをバックグラウンドで実行し、クライアントをウイルス感染から保護するアプリケーションです。G Data Security Client は、G Data Administrator 経由でリモートインストールできます。
- **G Data BootCD Wizard**: G Data BootCD Wizard を使うと、ブート可能かつベーシックなスキャン実行できるメディアを作成できます。BootCD ウィザード では最新ワクチンを適用したブートメディアを作成でき、これを使う事で OS 起動前にウイルススキャンを実行できます。製品 DVD を購入された場合は、この DVD をブートスキャンに利用できます。
- **G Data WebAdministrator**: G Data WebAdministrator は、ウェブベースの管理用プログラムです。G Data ManagementServer 用の設定の作成や編集をウェブ経由で操作することができます。
- **G Data MobileAdministrator**: G Data MobileAdministrator は、モバイル端末用に最適化した G Data ManagementServer 用のコントロールパネルです。あらゆるモバイルブラウザを使って起動でき、G Data Administrator の主要機能を利用できます。G Data MobileAdministrator は、G Data のすべての法人製品で利用できます。

インストールの流れ

本製品のインストールは以下の手順で行います。脅威へ即対応する必要がある場合は、以下の手順の前に、感染の危険があるPC上で G Data ブートスキャン を実行してください。

1 まず、G Data ManagementServer をインストールしてください。最適の保護を提供するため、G Data ManagementServer は、常時ワクチンを自動でダウンロードできるように、常時稼動させてインターネットに接続状態にしておきます。G Data ManagementServer はサーバーOS以外にもインストールできます（動作環境を参照）。G Data ManagementServer をインストールすると、管理コンソールの G Data Administrator も一緒にインストールされます。

2 インストーラーの指示に従い、製品登録を行ってください。製品登録を行わないとワクチンおよびプログラム更新を利用できません。

3 G Data Administrator を起動すると、**サーバーセットアップ ウィザード**が自動起動します。これを使うと、G Data Security Client をネットワーク内のクライアントに簡単にリモートインストールできます。 サーバーセットアップ ウィザードで行った設定は、後からも変更できます。

> リモートインストールで問題が発生した場合は、Active Directory 同期 または製品メディアやインストールパッケージを使ってローカルインストールすることもできます。インストールパッケージは、グループポリシーオブジェクトやログオンスクリプトを使って配布できます。G Data ManagementServer をインストールしたコンピュータにも、G Data Security Client をインストールしてください。

4 サーバーセットアップとネットワーク内のクライアントへのインストール完了後は、G Data ウイルスガードによるリアルタイム保護やスキャンジョブ設定などのウイルス保護機能やワクチン/プログラム更新を、G Data Administrator 経由で一括管理できるようになります。

> G Data Administrator は、ネットワーク内であれば、どのクライアントにもインストールできます。そのため、サーバーが物理的に離れた位置に存在する環境などで、クライアント上で設定関連に問題が発生した場合は、クライアントに直接 G Data Administrator をインストールして、問題解決することもできます。また、ネットワーク外部から問題を解決する必要がある場合は、あらゆるブラウザで使用できる G Data WebAdministrator を使用してください。さらに、G Data MobileAdministrator を使うと、モバイルブラウザ経由で G Data 法人版製品のステータス確認や設定を行うことができます。

動作環境

本製品は、次の要件を満たす環境でご利用ください。

動作環境：Windows
G Data ManagementServer / G Data Security Client /
G Data Administrator / G Data Web Administrator / G Data Mobile Administrator

OS:	Windows 8 (32bit/64bit) Windows 7 (32bit/64bit) Windows Vista (32bit/64bit) Windows XP (32bit) [SP3以降] Windows Server 2003/2003 R2 (32bit/64bit) Windows Server 2008/2008 R2 (32bit/64bit) Windows Server 2012 (64bit) (各日本語版) ※Itaniumベースのエディションはサポートしていません。 ※これらのOSの各種エディションは、特に断りのない限りすべてサポートしています。 ※G Data Mobile AdministratorはWIndows 7/8, WIndows Server 2008R2/2012 に対応しています。
CPU:	Windows XP以外： 各OSの推奨速度以上 [1.5GHz以上を推奨] Windows XP： Pentium III 500MHz以上 [1GHz以上を推奨] ※ManagementServerとして使用するPCではマルチコアCPUを推奨
HDD:	2GB以上の空き容量 [3GB以上を推奨]
メモリ:	1GB以上の空き容量※ ※ManagementServer として使用するPCでは4GB以上の搭載メモリを推奨。管理するクライアント数によっては、推奨以上のメモリ容量が必要です。
その他:	TCP/IP プロトコルを使用できるネットワーク環境 インターネット接続

動作環境：Android
G Data InternetSecurity for Android

OS:	Android 2.1 以上
端末容量:	14MB以上の空き容量

動作環境：Linux

OS:	**Sambaプラグインのみ対応：** Ubuntu 8.04 - 9.04 Debian 4.0 - 6.0.3 SLED/SLES 10 SP2 - 11 Fedora 7 - 14 **簡易GUIクライアント版、Sambaプラグイン両対応：** Debian 5.0 - 6.0.3 OpenSuSE 11.3 - 11.4 Fedora 14 ※全て32 bit(i386)のみ対応
CPU:	1GHz以上 [1.5GHz以上を推奨]
HDD:	2GB以上の空き容量 [3GB以上を推奨]
メモリ:	512MB以上 [1GB以上を推奨]

? SMBプロトコル経由で複数のWindowsクライアントと共有されているLinuxコンピューター（ファイルサーバーとして稼動）には、専用の保護モジュール（Sambaプラグイン）をインストールできます。このモジュールは、ファイルにアクセスする度にスキャンを実行し、Samba サーバー からWindowsクライアント（またはWindowsクライアントからSamba サーバー）へのウイルス流入を防止します。

ポート構成

G Data 法人版製品では、セキュアなネットワーク通信用に複数のTCPポートを使っています。ファイアウォールを導入済みの場合は、以下のポートがファイアウォールの設定で許可されていることを確認してください。

メインサーバー (MMS)

- Port 7161 (TCP): クライアントおよびサブネットサーバーとの通信
- Port 7182 (TCP): G Data Administratorとの通信
- Port 7183 (TCP): モバイルクライアントとの通信
- Port 7184 (TCP): モバイルクライアントとの通信（インストールファイルの配布用）

サブネットサーバー

- Port 7161 (TCP): クライアントおよび（サブネット）サーバーとの通信

クライアント

- Port 7167 (TCP): （サブネット）サーバーとの通信
- Port 7169 (TCP): クライアントとの通信 (ピアツーピア更新配布)

ポートの変更

G Data 法人製品でデフォルト設定のポート番号は、標準的なアプリケーションとの干渉を避けるように選択されたものです。しかし、ポートの干渉が発生した場合のために、G Data ManagementServer のポートは変更することもできます。

ポートを変更するには、管理者権限で Windows のサービス管理ツールを起動し (Start, Run, *services.msc*) 、G Data ManagementServer を停止します。次に G Data のインストールフォルダ（通常C:\Program Files\G DATA\G DATA AntiVirus ManagementServer）に移動し、メモ帳などのテキストエディタで gdmms.exe.config を開きます。変更が必要なポートを、以下のエントリで変更できます。

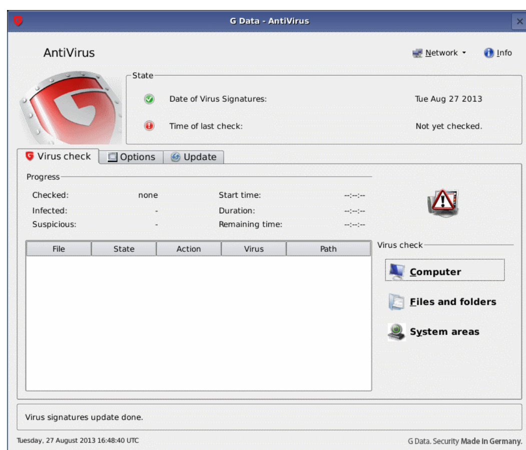
- AdminPort: デフォルト値は "0" です。この値を "0" のままにしておくと、Port 7182が適用されます。
- ClientHttpsPort: デフォルト値は "0" です。この値を "0" のままにしておくと、Port 7183 が適用されます。モバイルクライアントは、Port 7183 以外のポートは受け付けないため、通常、ClientHttpsPort の値は変更しないでください。
- ClientHttpPort: デフォルト値は "0" です。この値を "0" のままにしておくと、Port 7184 が適用されます。

ClientHttpPort もしくは ClientHttpsPort の値を変更すると、各ポートのHTTPSセキュリティ構成を新たに初期化する必要があります。これを行うには、管理者権限でコマンドプロンプトを開き、*C:\Program Files\G DATA\G DATA AntiVirus ManagementServer\gdmmsconfig.exe /installcert* を起動してください。

ポート変更後は、G Data ManagementServer を再起動します。なお、AdminiPortを変更した場合は、G Data Administrator のログイン時に毎回、次のフォーマットで変更したポートを指定する必要があります。フォーマット: *servername:port*

G Data Boot CD

感染が疑われるコンピュータへのインストール、また感染済みのウイルスによって G Data 法人製品のインストールがブロックされる場合は、G Data BootCD を使って、OS起動前にウイルススキャンを実行してください。



1a **製品メディアを使った方法**: G Data 法人製品の製品メディアをCD/DVDドライブにセットします。自動再生が有効な場合は、スタートウィンドウが表示されるので、 **［キャンセル］** を押してから、コンピュータをシャットダウンします。

1b **自身で作成した G Data BootCD を使った方法**: G Data BootCD の作成は、G Data BootCD Wizard 経由で行います。G Data BootCD Wizard を、G Data Security Client がインストール済みで最新ワクチンが配布されているコンピュータで実行してください。G Data BootCD のインストール後は、 画面の手順に沿って BootCD の作成を進めてください。 作成が完了したら、BootCD を対象コンピュータのCD/DVDドライブにセットします。

2 コンピュータを起動します。G Data BootCD のスタートメニューが表示されます。

3 矢印キーを使って、**G Data BootCD** のオプションを選択します。次に **Enter** キーを押します。BootCD内に収められているLinux OSが起動し、G Data BootCD のインターフェースが表示されます。

G Data BootCD のインターフェースの表示に問題がある場合は、コンピュータを再起動し、**G Data BootCD – alternative** のオプションを選択してください。

4 ワクチン更新を実行するかどうかをプログラムに尋ねられるので、 **［はい］** を選択して更新を実行します。更新が完了すると、 **更新しました。** のメッセージが表示されます。 **［閉じる］** を押して、更新画面を終了します。

IPを自動割り当てするルーター（DHCP）を使用している場合、インターネット更新が利用できます。インターネット更新が利用できない場合は、古いワクチンを使ってブートスキャンを実行できますが、G Data 製品のインストール後、早めに最新ワクチンで再スキャンすることをお勧めします。G Data BootCDを自身で作成した場合、BootCD内のワクチンバージョンは、作成元コンピュータにインストールされている G Data Security Client が作成時点で保持していたものとなります。

5 プログラムインターフェースが表示されます。スキャン領域の **コンピュータ** をクリックして、ウイルススキャンを実行します。ウイルススキャンの所要時間は、コンピュータの種類や保存領域のサイズによって変化しますが、通常、一時間かそれ以上掛かります。

6 ウイルスが検出された場合、プログラムによって提案された操作を使って、ウイルスを駆除してください。ウイルス駆除に成功すると、感染ファイルはもと通りの状態で利用できるようになります。駆除できないウイルスの場合は削除する事もできます。※削除したファイルは復元できませんので、この操作は注意して行ってください。

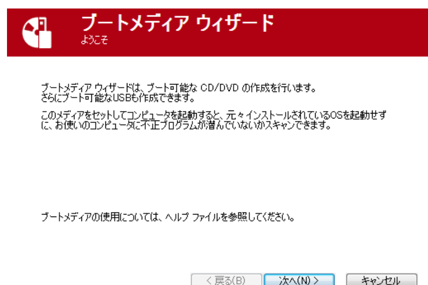
7 .スキャン完了後はウインドウ右上の X**ボタン** もしくは、ウインドウのタイトルを右クリックした後に［**close**］を選択し、次に［**再起動**］を選択してください。

8 G Data BootCD をCD/DVDドライブから取り外します。

9 コンピュータを再起動すると、通常のOSが起動します。これで、G Data 製品をウイルスフリーの環境にインストールする準備が整いました。

Boot CD の作成

G Data BootCDを作成するには、まずG Data BootCD Wizard をインストールする必要があります。G Data BootCD Wizard は、G Data Security Client がインストールされていて、かつ最新ワクチンが配布されているコンピュータにインストールしてください。G Data 製品メディアをセットし、［**インストール**］ ボタンを押します。次に、［**G Data BootCD Wizard**］ を選択します。



インストール後は、 **Create BootCD** （**スタート** > **(すべての) プログラム** > **G Data** > **G Data BootCD Wizard**） からBoot CD Wizard を起動できます。ウィザードでは、G Data BootCD のイメージファイルを作成できます。BootCDのイメージに最新ワクチンを適用するために、ワクチン更新を実行してください。ワクチンの更新後は、BootCDを特定のドライブに書き込むか、ISOイメージとして保存するか、選択できます。ISOファイルをCDに書き込むには、別途、書き込み用ソフトが必要です。

CD/DVD ブートの有効化

コンピュータをCD/DVDから起動できない場合は、BIOS設定でCD/DVDからの起動を有効にしてください。設定は以下の方法で変更できます。

1. コンピュータをシャットダウンします。

2. コンピュータを起動し、**DEL** キーを押してBIOS設定を呼び出します。コンピュータによっては、DELキーの代わりに **F2**、**F10**、**F12** キーが割り当てられている場合があります。 詳細は、ご利用のコンピューターの取扱説明書を参照してください。

3. BIOSセットアップの設定方法については、ご利用のコンピューター（もしくはマザーボードメーカー）の取扱説明書を参照してください。ご利用のコンピューター（もしくはマザーボードメーカー）の取扱説明書を参照し、**CD/DVD-ROM, C:** を1st Boot Device（ブート順序で1番目）に設定します。Windows OSが収められている記憶領域は、2nd Boot Device （ブート順序で2番目）に設定してください。

4. .変更を保存し、コンピュータを再起動します。これで、ブートスキャンの準備が整いました。

G Data ManagementServer のインストール



G Data ManagementServer をインストールするには、本製品の製品メディアをセットし、［**インストール**］ ボタンを押します。次に、［**G Data ManagementServer**］ のボタンを選択します。

インストール先のコンピュータ上で、アプリケーションがすべて閉じられていることを確認してください。アプリケーションを開いた状態でインストールを行うと、問題が発生する場合があります。次に、使用許諾契約書の内容をよく読み、**使用許諾契約の条項に同意します** を選択して、［**次へ**］をクリックします。続いて、インストール先フォルダを選択します。保存先を変更するには、[**変更**]を選択してください。

<u>**サーバータイプを選択**</u>

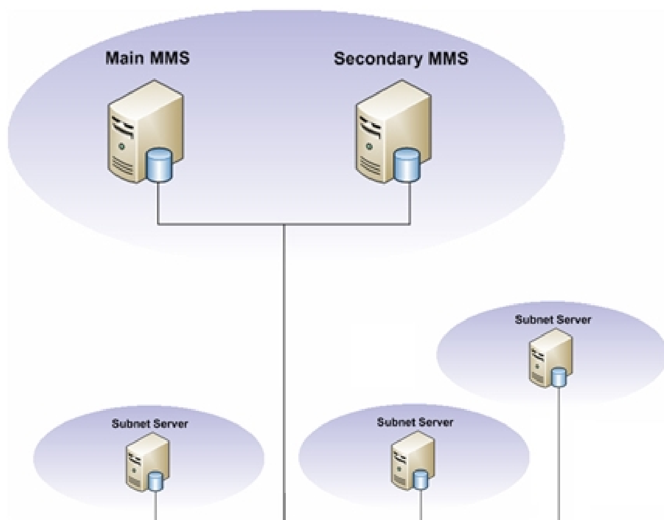
サーバーの種類は、以下から選択できます。

- **メイン サーバーをインストール**: G Data ManagementServer の初回インストール時は、必ずこのオプションを選択します。メインサーバーは、保護アーキテクチャの中核をなす管理インスタンスとして機能し、ワクチンやプログラムの更新ファイルをクライアントに配布したり、クライアントの設定や操作を中央管理します。

- **セカンダリ サーバーをインストール**: SQLデータベース を使用する環境では、メインサーバーと同一データを保持するセカンダリサーバー（Secondary-MMS）を設置することができます。メインサーバーが1時間以上接続不能なダウン状態に陥ると、クライアントは自動的にセカンダリサーバーに接続を切り替え、セカンダリサーバーから更新をロードします。メインサーバーの復旧後は、クライアントの接続は自動的にメインサーバーに切り替わります。セカンダリサーバーのワクチン更新は、メインサーバーに依存せずに、ダイレクトに G Data の更新サーバーからロードされます。

- **サブネット サーバーをインストール**: 大規模ネットワーク環境では、サブネットサーバーの導入をお勧めします。サブネットサーバーを導入すると、クライアントとメインサーバー間のトラフィックを分散でき、メインサーバーへの負荷を大幅に削減できます。サブネットサーバーは、メインサーバーやセカンダリ サーバーが接続不能な状況下でも、独立して稼動し続けます。ワクチン更新は、セカンダリサーバーのケースとは異なり、メインサーバー経由で行われ、専用のデータベースは必要ありません。

大規模ネットワークにおけるサーバーの種類の構成概要は、以下のようになります。サブネットサーバーが個々のクライアントまたはクライアントグループを束ね、それぞれのサブネットサーバーは、メインサーバーに接続されています。メインサーバーがダウンした場合は、サブネットサーバーは、メインサーバーからセカンダリサーバーに接続が切り替わります。大規模ネットワークでは、ピアツーピアによる更新配布で大きなパフォーマンスUPを図ることができます。ピアツーピア更新配布を有効にすると、更新によるサーバー・クライアント間の通信を大幅に削減できます。ネットワークによっては、ピアツーピア更新配布の有効化で、サブネットサーバーの導入が不要になることもあります。



データベース サーバー

G Data ManagementServer が使用するデータベースサーバーの種類を以下から選択します。

- **Microsoft SQL-Express**: 管理対象が300台未満で、G Data 法人製品を始めてインストールする場合、または利用できるSQL-Serverが無い場合に選択します。

  このオプションを選択して [次へ]を押すと、Microsoft SQL Express の使用許諾契約が表示されるので、**使用許諾契約の条項に同意します**を選択し、[次へ]をクリックします。次の画面では、［インストール］を押すとインストールを開始します。Microsoft SQL ExpressはG Data 法人版製品に同梱されています。

- **既存のSQL-Server インスタンス**: 既存のSQL-Serverを利用して大規模ネットワーク（300台以上に推奨）を管理する場合や既存のSQL-Expressデータベースを利用する場合に選択します。

製品登録（アクセスデータの入力）

インストール中に認証を行うことができます。

- **レジストレーション番号を登録**: 新規購入された方は、ここを選択し、購入製品のレジストレーション番号を入力してください。認証に成功すると、画面上にアクセスデータ（ユーザー名とパスワード）が表示されます。アクセスデータはメモをして厳重に保管してください。アクセスデータはプログラムに自動的に保存されます。

  ユーザー認証を行うには、インターネット接続が必要です。

レジストレーション番号は初回登録時にのみ使用します。

入力したレジストレーション番号で認証できない場合は、入力ミスの可能性がないか確認してください。それでも問題が解決できない場合は、ユーザーサポートまでお問い合わせください。

- **アクセスデータを入力**: アクセスデータ（ユーザー名とパスワードを使って、認証します。本製品を再インストールする場合は、ここを選択してアクセスデータを入力してください。
- **後で認証を行う**: 手元にアクセスデータが見つからない場合は、ここを選択します。なお、認証を行わないと、更新が利用できず最新の脅威から守ることができません。インストール完了後、できるだけ速やかに認証を実行してください。認証のやり方はこちらを参照してください。

注意: **後で認証**を行うを選択して製品をインストールした場合、G Data ClientSecurity Business/G Data EndpointProtection Businessを購入されていてもG Data AntiVirus Businessのみがインストールされます。 G Data ClientSecurity Business/G Data EndpointProtection Businessに含まれるファイアウォールやポリシーマネージャーの機能は、認証完了後に効化され利用できるようになります。

G Data ManagementServer の設定

このインストールステップは、G Data ManagementServer の再インストールもしくはSQLデータベースがコンピュータにインストール済みの場合にのみ表示されます。**設定をテスト**を実行して問題が無ければ、［**閉じる**］ボタンを押して閉じてください。

インストール完了後

G Data ManagementServer のインストール後、再起動が必要になる場合があります。管理コンソールの**G Data Administrator** を起動するには、**スタート** > **(すべての) プログラム** > **G Data Administrator** へ移動して **G Data Administrator** を選択するか、デスクトップ上のアイコンをクリックします。

G Data Administrator のインストール

G Data ManagementServer のインストール先には、G Data Administrator も自動的にインストールされます。G Data Administrator は、クライアントPCにもインストール可能です。必要に応じてインストールしてください。



G Data Administratorをインストールするには、本製品の製品メディアをセットし、［**インストール**］ ボタンを押します。次に、［**G Data Administrator**］ のボタンを選択します。

起動中のアプリケーションをすべて閉じていることを確認してください。アプリケーションを起動したままインストールを続行すると、インストールが正常に行われない場合があります。**[次へ]** ボタンをクリックし、インストール ウィザードに従って、インストールを続行します。インストール完了後、**G Data Administrator** は、デスクトップ上に作成されたアイコン、もしくは**スタート** > **(すべての) プログラム** > **G Data** > **G Data Administrator** から起動できるようになります。

G Data WebAdministrator のインストール



G Data WebAdministratorをインストールするには、本製品の製品メディアをセットし、［**インストール**］ ボタンを押します。次に、［**G Data WebAdministrator**］ のボタンを選択します。

G Data WebAdministrator のインストール方法はシンプルです。使用許諾契約書に同意した後、インストール先のフォルダを選択してください。推奨の保存先は、ウェブサーバーのHTTPフォルダです（例: \inetpub\wwwroot）。

インストール先環境によっては、G Data WebAdministrator のインストール中に追加のソフトウェア（下記参照）をインストールすることを求められることがあります。

- **インターネット インフォメーション サービス (IIS)**: WebAdministrator はウェブベースの製品のため、インストール先のコンピュータは、ウェブサーバーとして機能する必要があります。WebAdministrator は、**インターネット インフォメーション サービス (IIS)** をサポートしています。**WebAdministrator のインストール前に IIS が動作していることを確認してください。**
- **IIS 6 メタベース互換**: WebAdministrator をインストールする前に、IIS サーバー上で **IIS 6 メタベース互換** が有効になっているか確認してください。これが有効になっていないと、WebAdministrator はインストールできません。Windows 7 では、**スタート** > **コントロールパネル** > **プログラム** > **プログラムと機能** > **Windows の機能の有効化または無効化** に移動します。次に表示される **Windows の機能** のウィンドウで、**インターネット インフォメーション サービス** > **Web 管理ツール** > **IIS 6 と互換性のある管理** 内の **IIS メタベースおよび IIS 6 構成との互換性** のチェックボックスがオンになっていることを確認してください。また、**インターネット インフォメーション サービス** > **World Web Wide サービス** で **World Web Wide サービス** のチェックボックスがオンになっていることも確認してください。サーバー版OSを使用している場合、同様のオプションが **サーバーマネージャーの役割**タブで **IIS 6 メタベース互換** がインストールされていることを確認してください。
- **Microsoft .NET Framework**: WebAdministrator は、Microsoft .NET Framework ベースで構築されたアプリケーションです。Microsoft .NET Framework がインストールされていない場合は、インストール ウィザードによって Microsoft .NET Framework のインストールが求められます。インストール後は再起動が必要となります。

- **Microsoft Silverlight**: WebAdministrator の動作には、Microsoft Silverlight が必要です。Silverlight が未インストールの場合には、WebAdministrator の初回起動時にユーザーに通知します。

  ※ 主にWinsows 8 において、ログイン画面が表示され、各種情報を正確に入力しているにも関わらず、WebAdministrator にログインできない場合は .NET Framework 4.5 の機能有効化が不十分な場合があります。
  Windowsの機能の有効化または無効化画面から、.NET Framework 4.5 の階層を開き、WCFサービス 以下の HTTPアクティブ化、TCPアクティブ化、TCPポート共有にチェックが入っているかを確認してください。



インストール完了時には、WebAdministrator へのアクセス用アドレスがダイアログで表示され、デスクトップ上も G Data WebAdministratorのアイコンが作成されます。このアイコンをクリックすることで、G Data WebAdministrator を簡単に起動できるようになります。

安全なインターネット接続が確保されていない環境下での WebAdministrator の使用は、潜在的なセキュリティリスクとなります。セキュリティのためにも、IIS で SSL サーバー証明書を構成することをお勧めします。

G Data MobileAdministrator のインストール



G Data MobileAdministratorをインストールするには、本製品の製品メディアをクライアントPCのDVDドライブにセットし、［**インストール**］ボタンを押します。次に、［**G Data MobileAdministrator**］ を選択します。

G Data MobileAdministrator のインストールは、WebAdministrator と同様の流れで行うことができます。使用許諾契約書に同意した後、MobileAdministrator のインストール先フォルダを選択します。推奨の保存先は、ウェブサーバーのHTTPフォルダです（例: \inetpub\wwwroot）。

G Data MobileAdministrator のインストール中は、追加のソフトウェアをインストールすることを求められることがあります。MobileAdministrator には、以下の要件が必要となります。

- **Microsoft Windows 7/Microsoft Windows Server 2008 R2 以降のOS**: MobileAdministrator のインストールは、Windows 7 もしくは Windows Server 2008 R2 以降のOSが必要となります。
- **インターネット インフォメーション サービス (IIS)**: MobileAdministrator はウェブベースの製品のため、インストール先のコンピュータは、ウェブサーバーとして機能する必要があります。MobileAdministrator は、インターネット インフォメーション サービス (IIS)をサポートしています。**MobileAdministrator のインストール前に IIS が動作していることを確認してください。**

- **Microsoft .NET Framework**: Microsoft .NET Framework ベースで構築されたアプリケーションです。Microsoft .NET Framework がインストールされていない場合は、インストール ウィザードによって Microsoft .NET Framework のインストールが求められます。インストール後は再起動が必要となります。

インストール完了後は、MobileAdministrator へのアクセス用アドレスがダイアログで表示されます。アクセスする際は、そのアドレスをブラウザに入力して使用します。

安全なインターネット接続が確保されていない環境下での MobileAdministrator の使用は、潜在的なセキュリティリスクとなります。セキュリティのためにも、IIS でサーバー証明書を構成することをお勧めします。

G Data Security Client のインストール

ネットワーク内のクライアントを保護・管理するには、G Data Security Client を各クライアントPCにインストールする必要があります。導入環境に応じて、リモートインストール (G Data Administrator経由) もしくはローカルインストール (製品メディアまたはクライアントインストール パッケージを使用)から選択してください。G Data Security Client は、クライアントPCだけでなく、サーバーにもインストールすることをお勧めします。

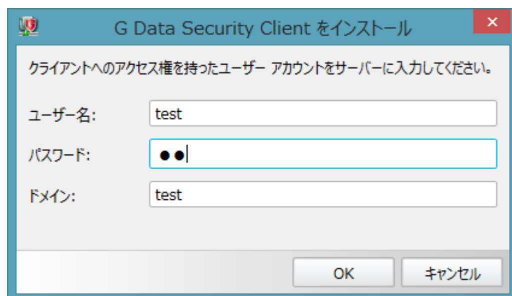
G Data Security Client をサーバーにインストールする際は、そのサーバーが行っている作業に支障が出ないよう注意をしてください。
例えば、データベースサーバーやメールサーバーなどではウイルスガードやスキャンジョブにおいて例外設定を設定、場合によっては、メールスキャンやインターネットコンテンツのスキャンなどは干渉を避けるため機能自体を無効にする。というように、環境によって支障がより少なくなる設定を行う必要があります。

リモートインストール

クライアント用プログラムである G Data Security Client のインストール方法の中でもっとも便利な方法は、 G Data Administrator を介したリモートインストールです。**サーバーセットアップウィザード** を使うと、G Data Security Client をネットワーク内の全マシンに一括インストールできます。

リモートインストールには、**ポート構成**の他に、以下の要件を満たす必要があります。

- ファイアウォールが導入されている環境では、gdmms.exe が例外に設定されていること。
- Windows ワークグループ環境では、「簡易ファイルの共有」（Windows XP）、または「共有ウィザードを使用する」（Windows Vista または Windows 7）のオプションが無効化されていること。さらに、「ユーザーアカウント制御（UAC）も無効化されていること。
- 対象クライアントの管理共有フォルダ（「C$」 および 「Admin$」）へのアクセスが可能なこと。
- パスワードが設定されていること（空のパスワードは無効）。
- 「リモート レジストリ サービス」が「サービス」で有効化されていること。



G Data Administrator の初回起動時に自動起動する **サーバーセットアップ ウィザード** を使うと、ネットワーク内のログオンしているコンピュータの一覧が表示されます。コンピュータは名前をマニュアル入力して追加し、有効にすることができます。次に、有効化されたクライアントを選択して右クリックします。表示されるメニューの中から **G Data Security Client をインストール** を選択します。そうすると、クライアントへアクセス可能な**ユーザー名、パスワード** および**ドメイン**を入力するウィンドウが表示されます。表示言語の選択後に、G Data Firewall も一緒にインストールするか確認のメッセージが表示されます（G Data ClientSecurity Business および G Data EndpointProtection Business のみ）。ダイアログウィンドウでインストールの進捗状況が表示されます。インストール完了後は、クライアントの再起動が必要になります。

Active Directory 統合 を使用している場合は、新たに追加したコンピュータに G Data Security Client を自動インストールできます。

リモートインストールの実行は、次の2種類に分かれます。クライアントがすべての要件を満たている場合は、インストールファイルがクライアントＰＣにコピーされ、インストールが実行されてレジストリエントリに書き込みが行われます。クライアントＰＣのレジストリへアクセスが不可能な場合、あるいはシステム要件が満たされていない場合は、セットアッププログラムはクライアントにコピーされて、クライアントＰＣの次回起動時にインストールが行われます。

クライアントプログラムがリモートインストールでインストールできない場合は、製品ＤＶＤもしくはインストールパックを使ってローカルインストールをしてください。インストールパックは、ログオンスクリプトまたはグループポリシーオブジェクト（ＧＰＯ）経由で配布することもできます。

ローカルインストール

リモートインストールができない場合は、G Data Security Client をクライアント上でローカルインストールできます。ローカルインストールを実行するには、製品メディアもしくはインストールパッケージを利用してください。多くのクライアントに配布する必要がある場合、インストールパッケージはログオンスクリプトを利用して配布することをお勧めします。

製品メディアを利用したインストール



本製品の製品メディアをクライアントPCのDVDドライブにセットし、**［インストール］**ボタンを押します。次に、**［G Data Security Client］** を選択します。

インストール中に、サーバー名もしくは G Data ManagementServer のインストール先サーバーのIPアドレスを入力してください。サーバー名は、クライアントがサーバーと接続するために必要です。

インストールパックを利用したインストール



インストールパッケージは、クライアントユーザーによるインストール操作が一切不要なバックグラウンドインストールが行われる実行ファイル (GDClientPck.exe)です。インストールパッケージは、ログインスクリプト経由でドメインに属する全クライアントＰＣへ配布したり、ローカルでのインストールに適しています。G Data Administrator で作成されたインストールパックには、G Data Security Client の最新バージョンが適用されます。

インストールパッケージを作成するには、まず G Data Administrator を起動します。 **組織** メニューから、**G Data Security Client のインストールパックを作成** を選択します。次に、クライアントの管理先ManagementServer とプログラムでの言語を選択して［OK］をクリックします。次の画面で、作成したインストールパックの保存先を選択すると、G Data Administrator がインストールパッケージの作成を開始します。作成したインストールパックは、インストール先クライアントにコピーして、管理者権限で実行する必要があります。インストールパックによるインストールは、バックグラウンドで行われるため、ユーザー側の操作は一切必要ありません。

※ ファイアウォールを使用できる製品の場合、上記の方法でインストールを行った後 G Data ManagementServer でファイアウォールをインストールするまでは、ファイアウォールの機能が有効になりません。最初からファイアウォールを含めてインストールしたい場合は、製品メディアもしくはインストールパックのショートカットを作成した後、ショートカットのプロパティを開き、リンク部分に以下のオプションを追加してから実行してください。

製品メディアからのインストールの場合: /v"INSTALLFW=yes"

インストールパックからのインストールの場合: /fw

Linux クライアントのインストール

Linux クライアントは、Windows 用クライアントと同じように、G Data ManagementServer に接続でき、設定やワクチン更新などを G Data Administrator 経由で中央管理できます。

ファイルサーバーとして稼動し、Windows 共有（SMBプロトコル経由）を提供する Linux マシンには、専用モジュールの Security Client for Linux FileServer をインストールできます。このモジュールは、共有ファイルへのアクセスを制御し、Samba サーバーから Windows クライアント（または Windows クライアントからSamba サーバー）へのマルウェア感染がおこらないように、ファイルアクセスの度にスキャンを実行します。

Linux Workstation クライアントは、ディストリビューションのカーネルバージョンが 2.6.25以降である必要があります（例: Debian 5.0, OpenSuSE 11.3など）。
※カーネルバージョンの条件を満たしていても動作しないディストリビューションもあります。詳しくは **動作環境** をご確認ください。

ファイルサーバー用クライアントは、上記以外のカーネルバージョンの制約を受けることなく、一般的に普及するディストリビューションであれば、使用することができます。

リモートインストール

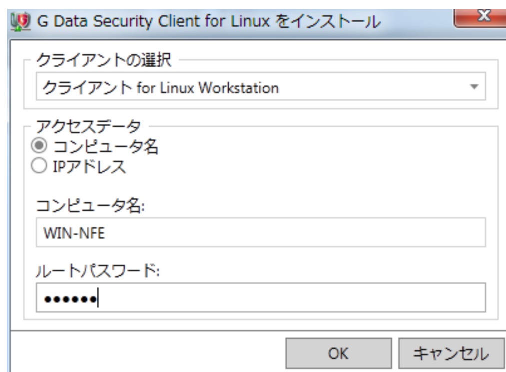
Linux クライアントへのリモートインストールは、以下の手順に沿って進めてください。

1. G Data Administrator の **クライアント** タブで、 一覧メニューを開き、対象クライアントを右クリック、**G Data Security Client for Linux をインストール** コマンドを選択してください。ダイアログウィンドウが表示されるので、インストールを行うクライアントの種類（FileServer もしくは Workstation）を選択します。
※クライアントマシンは、ネットワーク内で認識されている必要があります。

2. クライアントマシンにSamba サービスがインストールされている、もしくはネットワークのネームサーバーに登録されている場合は、**コンピュータ名**を選択します。コンピュータ名が不明の場合は、**IP アドレス** を使ってください。

3. コンピュータの **root パスワード** を入力してください。リモートインストールには、ルートパスワードは、設定する必要があります。特定ディストリビューションでは、root パスワードがデフォルトで設定されていない場合があります（例: Ubuntu）。

4. **[インストール]** ボタンを押してください。クライアントソフトのインストールが正常に実行されたかは、**ステータス** 領域で確認きます。



ローカルインストール

製品メディア内のディレクトリ **\Setup\LinuxClient** に以下のファイルがあります。

- **installer.bin** (Linux クライアント用インストーラー)
- **uninstaller.sh** (Linux クライアント用アンインストーラー)

これらのファイルをクライアントマシンにコピーし、 installer.binでインストールを開始します。インストール後は更新が自動実行されますが、必要に応じて、製品メディア内の以下のワクチン用ファイルをコピーすることもできます。

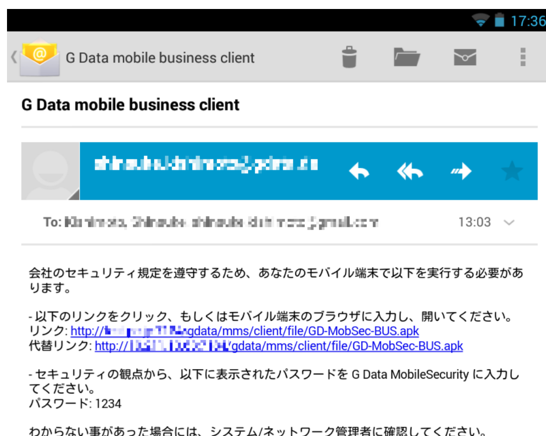
- **signatures.tar** (ワクチン用ファイル)

G Data Internet Security for Android のインストール

G Data 法人版では、Android端末用セキュリティアプリ G Data Internet Security for Android の法人版を統合することによって、Android端末の保護と端末の中央管理を行う事ができます。

モバイル端末へ G Data Internet Security for Android をインストールするには、G Data Administrator のクライアント管理領域へ移動し、**インストール用リンクをモバイルクライアントに送信** アイコンを選択（もしくは、クライアント選択領域で対象クライアント上で右クリック）します。これで、モバイルクライアントに G Data Internet Security for Android のダウンロードリンクを含むメールが送信されます。複数のメールアドレスを入力するには、アドレス入力後に改行するもしくはカンマ (,) を挿入します。

サーバー設定 > Mobile でパスワードをまだ入力していない場合は、**モバイルクライアント用認証** 欄にパスワードを入力してください。



メールを端末に送信した後は、G Data Administrator から送信したメールを端末上で開きます。次に、ダウンロードリンクをタップして、APKファイルのダウンロードを開始します。

注意: ダウンロードリンクからアプリをダウンロードするには、端末設定の**提供元不明のアプリ (提供元がPlayストアでないアプリのインストールを許可する)** のオプションが有効化されている必要があります。このオプションは、通常、**設定** > **セキュリティ** > **デバイス管理** もしくは **設定** > **アプリケーション** から確認できます。

APKファイルを開いて要求されたパーミッションを確認すると、G Data Internet Security for Android のインストールが始まります。インストール完了後は、アプリメニューから G Data Internet Security for Android を起動できるようになります。アプリを起動すると、画面左上の**設定**アイコンからリモート管理の許可を設定できます。 **リモート管理を許可する** にチェックを入れて、 **サーバーアドレス** に ManagementServer の名前もしくはIPアドレスを入力します。**端末名** では、G Data Administrator 上での端末表示名を割り当てることができます。**パスワード** では、G Data Administrator で入力されたパスワード（端末に送信されたメールにも記載されています）を入力してください。

すべての情報が問題無く設定した後にアプリ上で更新を行うと、端末が G Data Administrator の **クライアント** 画面上で表示されるようになり、G Data Administrator からの設定変更が可能になります。

注意: MobileSecurity をインストールした端末が自動で表示されない場合は、G Data ManagementServer に強制認証させるため、**端末を再起動**してください。

G Data ManagementServer

G Data ManagementServer は G Data 法人製品の中核を構成するモジュールです。G Data 更新サーバーから提供される、最新ワクチンやプログラムファイルの自動ダウンロード、クライアントへの配布、ウイルススキャンや設定変更などを一括管理します。

クライアントと G Data ManagementServer 間の通信は、TCP/IP で行われます。もし **G Data Security Client** がインストール済みのクライアントがオフラインの状態にある場合は、次のオンライン時にジョブや設定の同期が行われます。

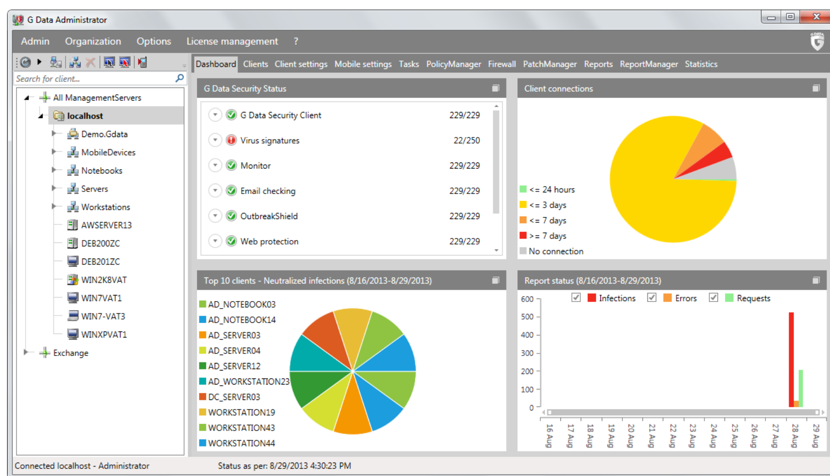
G Data ManagementServer は中央隔離フォルダ持っており、ウイルス感染の疑いがあるファイルは、暗号化して保存、削除、駆除、もしくは、必要に応じて G Data セキュリティラボへ送信できます。G Data ManagementServer の管理は、**G Data Administrator** 経由で行います。

※ G Data Administrator を終了しても、G Data ManagementServer は、引続きバックグラウンドで稼動し、設定されたプロセスを制御し続けます。

※ 作成された隔離フォルダの詳細パスは、**こちら**を参照ください。

G Data Administrator

G Data Administrator は、G Data ManagementServer の制御モジュールで、ネットワーク内のクライアントへのインストール・設定変更・各種操作など実行を行うことができます。G Data Administrator は、要件を満たす Windows OS を搭載するコンピュータであれば、ネットワーク内のどのコンピュータにでもインストールできます。なお、G Data Administrator はパスワード保護されているため、起動時にはパスワード入力を求められます。

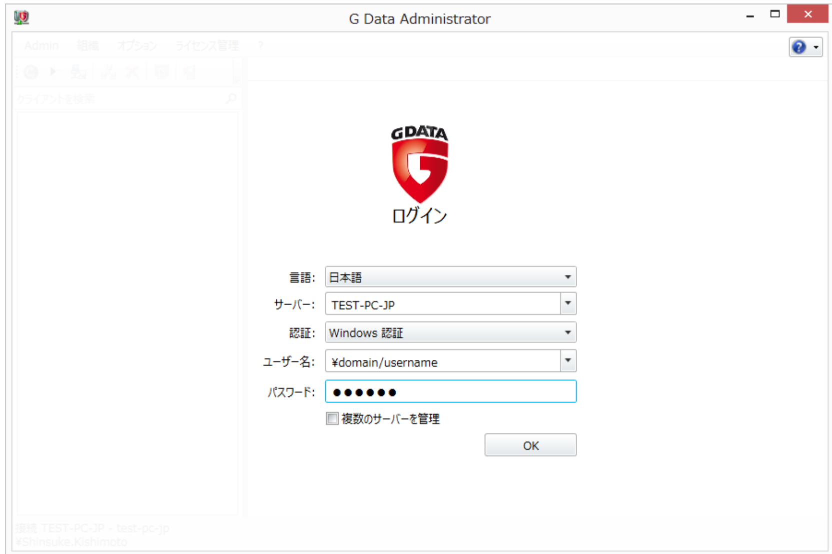


G Data Administrator　の画面左側の**クライアント選択領域**では、G Data Security Client がインストールされたコンピュータが階層表示されます。その右側の領域では、各項目のタブを選択すると、選択した項目の作業領域に切り替わります。作業領域の表示内容は、クライアント選択領域で選択されているクライアント（もしくはクライアントグループ）の情報が表示されます。クライアント選択領域および作業領域の上部にあるメニューバーとアイコンバーでは、モジュールに関する機能全般の操作や設定などを行います。

Samba サーバーとして機能する Linux クライアントの設定では、メールの処理を含む機能などはファイルサーバーに不要なため、予め変更できないように設定されています。Linux クライアントに設定できない機能は、機能の前に赤い点が表示されます。

G Data Administrator の起動

G Data Administrator は、インストール時に作成されたデスクトップアイコン、もしくは **[スタート]** > **[(すべての)プログラム]** > **[G Data]** > **[G Data Administrator]** を選択すると起動できます。



G Data Administrator を起動すると、まずログイン画面が表示されます。ログイン画面では、**言語、サーバー、認証、ユーザー名、パスワード** の欄が表示されます。サーバーの欄には、G Data ManagementServer がインストールされているコンピュータ名を入力してください。**認証**では、以下のいずれかを選択してください。

- **Windows 認証**: コンピュータの管理者権限を持つユーザー名とパスワード（Windowsユーザーアカウント）でログインを行います。G Data ManagementServer に SQL Server Express データベースをインストールした場合、Windows 認証を選択してください。
- **統合認証**: G Data ManagementServer 独自の認証方式です。この認証方式の場合、G Data ManagementServer でシステム管理者の権限を付与されたアカウントを使用する事でログインができます。このアカウントは G Data Administrator の**ユーザー管理**から設定や管理ができます。

G Data Administrator の設定

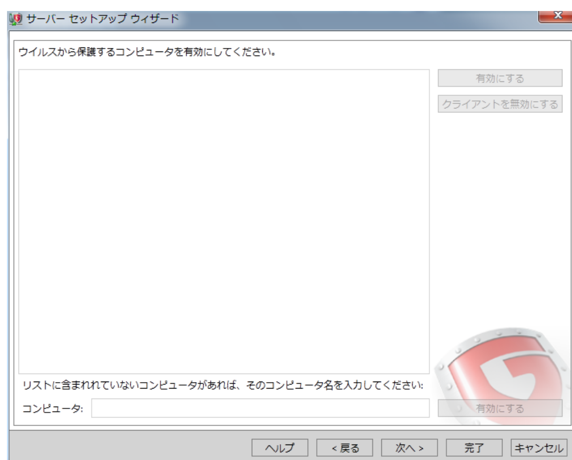
クライアントを細かく設定する前に、まずは重要な管理タスクを設定し、ご利用のネットワークに最適化してください。これは、サーバーセットアップから実行可能で、クライアントの有効化・インターネット更新設定・メール通知設定などが含まれます。サーバーセットアップは、G Data Administrator の初回ログイン時に表示されますが、G Data Administrator のメニューから**Admin**を選択することで、いつでも表示させることができます。

Admin

管理タスクに移動するには、G Data Administrator の **Admin** メニューを選択します。設定やインストール開始する前に、一度はこれらのタスクを実行しておくことをお勧めします。

サーバー セットアップウィザード

ダイアログ形式でクライアントを選択して、簡単な操作で対象クライアントを有効化する機能です。G Data Administrator の初回起動時には、このセットアップウィザードが自動的に開きます。一度設定が終わった後もメニューバーの **Admin** からいつでも呼び出すことが可能です。



クライアントを有効にする

G Data で監視するクライアントは、必ず有効化する必要があります。 クライアントを有効にするには、一覧で表示されるクライアントから対象を選択し、**[有効にする]** をクリックします。長い期間電源がオフになっているコンピュータ、ファイルやプリンタ共有が未設定のコンピュータは、一覧に表示されないことがあります。このようなクライアントを有効にするには、**[コンピュータ]** にクライアントのコンピュータ名を入力した後、その横の **[有効にする]** ボタンをクリックします。クライアントが有効になると、クライアント一覧に表示されます。すべてのクライアントを有効にしたら、**[次へ]** をクリックします。

インストール

次に表示される画面では、**有効にしたコンピュータに G Data Seurity Client を自動的にインストール** にチェックが入っています。他の方法（**インストールパック**もしくは製品メディア）を使用してインストールや後からインストールを実行する場合は、このチェックを外します。

インターネット更新

G Data ManagementServer は、インターネット経由で最新のワクチンやプログラムファイルをダウンロードします。自動更新を有効にするには、G Data 更新サーバーへの登録と自動更新の設定が必要です。オンライン登録時に受け取った**アクセスデータ**を入力してください。更新間隔の設定と基本的な設定手順の詳細は、 **インターネット更新**の項を参照してください。

インターネット更新の自動化は、G Data Administrator からも設定できます。

メール通知

メール通知は、特定のケース（**ウイルス検出時、ワクチンが古くなった場合、ファイアウォールによるブロック、ポリシーマネージャーの承認リクエスト**）などに指定したメールアドレス宛にメールを自動送信する機能です。メール通知を設定するには、まず**受信者グループ**を選択するか、歯車アイコンをクリックして、**メール設定**を開いてください。制限を設定すると、受信メールの数を**制限**できます。

- **ファイアウォールによるブロック**は、G Data ClientSecurity Business / G Data EndpointProtection Business にのみ含まれています。
- **ポリシーマネージャーの承認リクエスト**は、G Data EndpointProtection Business にのみ含まれています。

モバイル端末用の設定

モバイル端末用アプリのリモート管理を行う場合は端末上で**認証パスワード**の入力が必要です。そこで使用する認証パスワードと、盗難対策の緊急時の機能を利用する際に利用する Google Cloud Messaging 用の **送信者 ID** と **APIキー** を入力します。

すべての設定が完了したら、最後に **[完了]** をクリックして、設定ウィザードを閉じると設定完了です。

G Data Security Client の自動インストール

有効にしたコンピュータに G Data Seurity Client を自動的にインストール にチェックを入れた場合、有効なすべてのコンピュータに対し、G Data Security Client の自動インストールが始まります。G Data Security Client のリモートインストールが開始されます。

G Data クライアント をインストールの画面が開き、クライアントへのアクセス権を有するユーザーアカウント（ユーザー名とパスワード）の入力を求められます。有効なユーザー名とパスワードを入力して [OK] をクリックします。G Data ClientSecurity および G Data EndpointProtection ではファイアウォールを一緒にインストールする確認画面が表示されます。ファイアウォールを一緒にインストールする場合は、［**はい**］を選択してください。次に G Data Security Client の言語を選択画面が表示されるので、希望の言語を選択してから［OK］を押してください。

ログを表示

この画面では、実行した操作の概要を把握できます。各ログはフィルタすることにより項目別に表示できます。

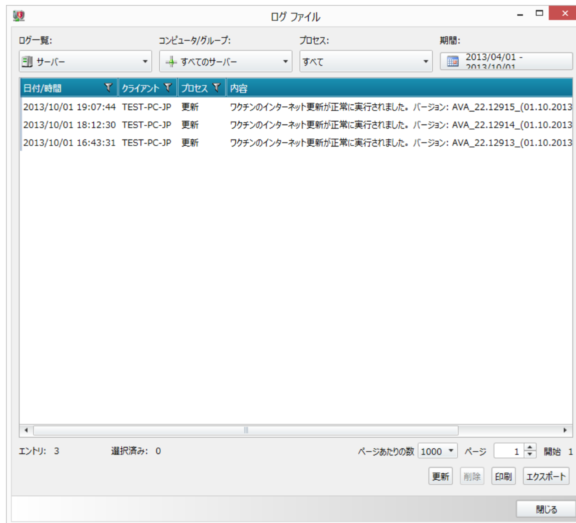
フィルタには次の4種類の項目があります。

- **ログ一覧**: クライアントまたはサーバーから選択できます。
- **コンピュータ/グループ**: すべてのクライアント、グループごと、または個々のクライアントから選択できます。
- **プロセス**: すべてのログ情報を表示させるか、特定のテーマに絞ったレポートのみを表示させるか、設定します。
- **期間**: ログを表示させる期間を設定します。

[**更新**] をクリックすると、ログファイル表示中に発生した最新プロセスも表示されます。有効なフィルタは小さな矢印マークで表示されます。

最初の表示画面では、すべてのプロセスは時系列順で表示されますが、ログ上部にある項目名をクリックすることで順番を並び変えることができます。

画面右下のボタンからは、各ログを XML ファイルとしてエクスポートしたり、印刷、削除する事ができます。



ユーザー管理

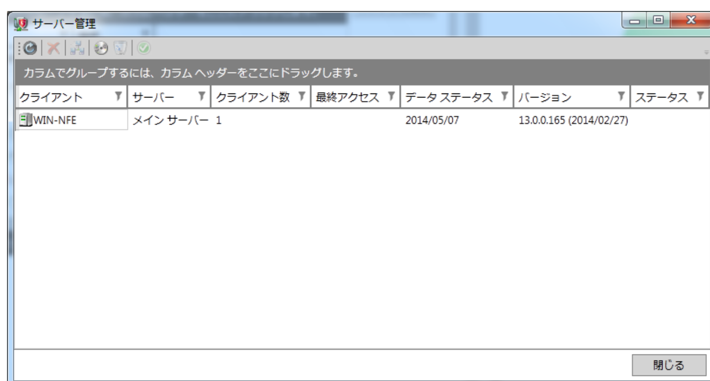
システム管理者は、G Data Administrator を利用するユーザーを追加できます。ユーザーを追加するには、**[新規]** をクリックしてください。次に表示されるウィンドウでは、 ユーザー名、権限 (**[読み取り / 書き込み]** または **[読み取り]**) 、アカウントの種類 （**[統合認証]**、**[Windows ユーザー]**、**[Windows ユーザーグループ]**）、パスワードを設定してください。



サーバー管理

サーバー管理では、個々のクライアントをサブネットサーバーに割り当てることができます。これにより、クライアントとメインサーバー間の通信を集約し、ネットワーク通信を最適化できます。サブネットサーバーをインストールするには、**[サブネットサーバーを追加]** をクリックします。**[クライアントを割り当て]** からは、既存のクライアントを指定のサブネットサーバーに割り当てることができます。

クライアントのサブネットサーバーへの割り当ては、クライアントのグループには何の影響も及ぼしません。そのため、異なるサブネットサーバーに割当てられた同一グループに属するクライアントには、サブネットサーバーへの割り当て後も、当該グループの設定が適用されます。



- **削除**: サブネットサーバーをリストから削除します。この操作を行うだけでは、インストール済みのプログラムは削除されません。
- **クライアントを割り当て**: クライアントをサブネットサーバーに割り当てします。
- **サブネットサーバーを追加**: 新しいサブネットサーバーを追加します。選択した後はダイアログが開くので、サブネットサーバーの**コンピュータ名**を入力します。次に、サブネットサーバー上で管理者権限を有するユーザーアカウントを入力します。**OK** ボタンを押して確定すると、リモートインストールが開始されます。インストールの状況は、**インストール概要**画面で確認できます。
- **サーバーをアンインストール**: サブネットサーバーのアンインストールを実行します。
- **認証を付与**: サーバーデータへの未承認アクセスを防ぐため、ローカルにインストールされたサブネットサーバーは認証を付与する必要があります。認証付与後、G Data ManagementServer はサブネットサーバーと同期できるようになります。

サブネットサーバーを追加 でリモートインストールを行ったサブネットサーバーは自動的に認証されます。サブネットサーバーをローカルインストールした場合や、旧バー

ジョンからver13へアップグレードした場合は手動で認証する必要があります。また、リモートでサブネットサーバーをアンインストールできるのは認証されたサブネットサーバーのみです。

サブネットサーバー同期

マネジメントサーバーとサブネットサーバー間の同期は、通常の通信間隔に自動同期されますが、この間隔以外に同期する場合は、**サブネットサーバー同期**から設定します。

終了

G Data Administrator を終了します。なお、G Data Administrator を終了した後も G Data ManagementServer は稼動を続け、ネットワーク内の G Data Security Client がインストールされたコンピュータは保護され続けます。

オプション

メニューバーのオプションでは、ManagementServerの機能に関連する各設定へ移動できます。オプションで利用できる設定の一部は、**サーバーセットアップ ウィザード** (例: **インターネット更新**) を呼び出して設定することもできます。

インターネット更新

ワクチンおよびプログラムファイル更新に関する設定、ステータス確認、および操作を実行します。**アクセスデータと設定**のタブを選択すると、オンライン登録時に受け取ったアクセスデータを入力できます。

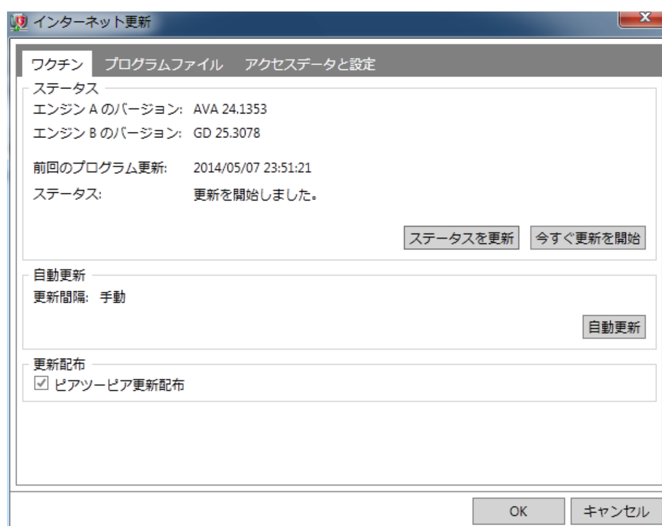
インターネット更新では、更新ファイルはまず G Data ManagementServer に保存され、そこから各クライアントへ配布されます。更新の配布は、**クライアント**の作業領域で操作します。

ワクチン

すべてのクライアントには、ワクチンファイルのコピーが保存されます。これによって、クライアントが G Data マネジメントサーバーと未接続、もしくはインターネットへ未接続のオフラインの状態でも、 システムをウイルスから保護できます。クライアントへの更新ファイルの配布プロセスは、次の2 段階のステップで行われます（2段階とも自動化が可能）。

第 1 ステップ: G Data 更新サーバー からの最新の更新ファイルがG Data マネジメントサーバー上のフォルダにコピー

第 2 ステップ: G Data マネジメントサーバー から更新ファイルがクライアントに配布 （クライアント設定を参照）



- **ステータスを更新**: クライアント側のワクチンのステータス表示を更新します（ステータス表示の変更が適用されていない場合）
- **今すぐ更新を開始**: ワクチン更新を今すぐに実行します
- **自動更新**: インターネット更新の自動実行を設定します。定期的に更新を実行にチェックを入れると、更新の実行スケジュールを設定できます。

  - 更新を自動的に実行するには、G Data マネジメントサーバー がインターネットに接続環境にあるか、G Data によるインターネットへの自動接続が設定されている必要があります。
  - 必要に応じて **アクセスデータと設定 > プロキシ設定** から設定を行ってください。

- **更新配布**: 更新ファイルは、ManagementServerからクライアント（サブネットサーバー導入環境ではサブネットサーバーを経由）に順々に配布する方式、もしくは **ピアツーピア更新配布方式**（クライアント経由の更新） が利用できます。ピアツーピア更新配布は、大規模ネットワークでの使用をお勧めします。

プログラムファイル（クライアント）

この画面ではG Data Security Client のプログラムファイル更新に関わる設定を行う事ができます。

クライアントのプログラム更新は、まずG Data 更新サーバー からG Data ManagementServer上のフォルダに、最新の更新プログラムファイルがコピーされた後、G Data ManagementServer からクライアントに更新ファイルが配布、インストールされます (**クライアント設定**を参照）。



- **ステータスを更新**: プログラムファイルのステータス表示を更新できます。

- **今すぐ更新を開始**: G Data ManagementServer が保持する G Data Security Client のプログラムファイル更新を今すぐに実行します。

- **自動更新**: インターネット更新も自動更新を設定できます。自動更新を設定するには、定期的に更新を実行にチェックを入れて、更新の実行スケジュールを設定します。

- 更新を自動的に実行するには、**G Data ManagementServer** がインターネットに接続環境にあるか、本製品によるインターネットへの自動接続が設定されている必要があります。必要に応じて **アクセスデータと設定 > プロキシ設定**からプロキシ接続用の設定を行ってください。

- G Data マネジメントサーバーのプログラムファイルを更新するには、**スタート > （すべての）プログラム > G Data > G Data ManagementServer > インターネット更新** から行います。G Data ManagementServer のプログラムファイルを更新する方法は、この方法が唯一の方法です。一方、G Data Security Client のプログラムファイル更新は、G Data Administrator から行うことができます。

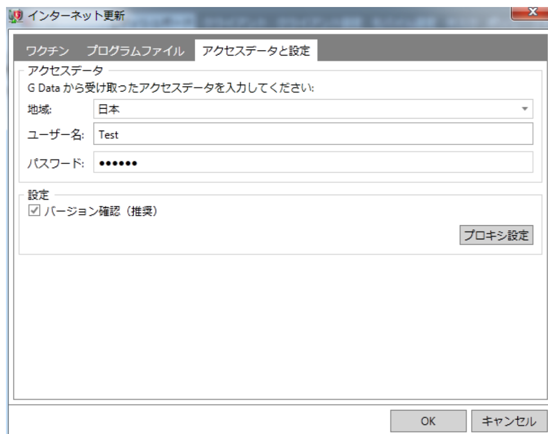
アクセスデータと設定

オンライン認証時に受け取ったアクセスデータを、**ユーザー名**および**パスワード**の欄に入力してください。

地域ではワクチンなどの更新用データを、どの地域のサーバーから取得するかを設定します。選択したサーバーとの距離により通信速度が変わりますので、日本国内で使用している場合は、日本を選択すると良好な速度が得られます。

バージョンチェック（デフォルトで有効）は、通常は常に有効にしておきます。これにより、増分の最新ワクチンだけがクライアントPCにコピーされるようになります。

ワクチン更新で問題が発生した場合、一旦バージョンの確認を無効にして更新を実行すると、問題が解決することがあります。



プロキシ設定では、インターネットおよびネットワークのアクセス用データを入力します。

この設定は、プロキシ環境での本製品の使用や、その他の標準的な設定で本製品をしている環境でインターネット更新に問題が発生し、更新を実行できない場合にのみ使用してください。

プロキシ設定では、プロキシサーバー環境用の設定を行います。設定を行うには、まず**プロキシサーバーを使用**にチェックを入れ、アドレス、ポート（デフォルト: 80）を設定します。プロキシサーバー用の**ユーザー名**、**パスワード**、およびプロキシサーバーの**アドレス**、**ポート番号**を設定できます。

- 本製品は、Internet Explorer (バージョン 4 以降) の接続データを使用できます。

1. まず Internet Explorer を設定して、以下のG Data 更新サーバーのテスト用サイトに到達できるか、確認します。

テスト用サイト

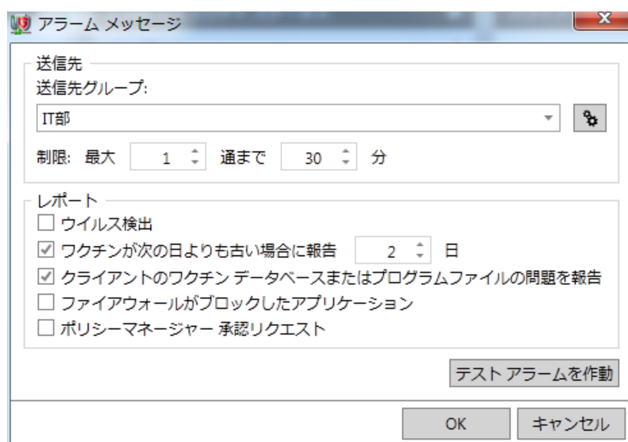
http://ieupdate.gdata.de/test.htm

2. テストサイトが正常に表示されたことを確認し、プロキシサーバーを使用をオフにします。

3. ユーザーアカウントには、 Internet Explorer で設定した対象のアカウントを入力します。

アラームメッセージ

アラームメッセージでは、ウイルス検出時に、G Data ManagementServer から**メール**で警告メッセージを自動送信するように設定できます。**ウイルス検出、ポリシーマネージャー 承認リクエスト**などのレポート方式を選択すると、メール通知は有効化されます。**送信先**では、メッセージを受信する**受信者者や受信者をまとめたグループ**を設定できます。**制限**からは受信メールの数量を制限できます。これを設定することで、大規模なウイルス検出が発生した場合などに受信者に大量のメールが送信されないように回避できます。制限は必ず設定することをお勧めします。



歯車アイコン () をクリックすると、受信者グループ設定用の **メール設定** ウィンドウが開きます。

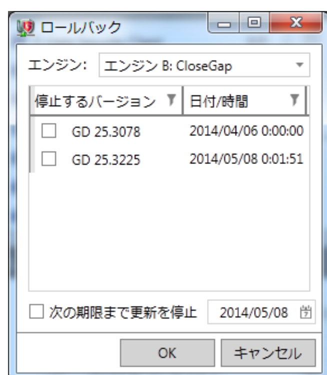
更新のロールバック

G Dataで使用されているワクチンのバージョンを過去のバージョンに置き換える機能です。この機能は、最新ワクチンを使用している環境において、誤検出が発生した際などに、誤検出前の状態にワクチンを戻すことができ、誤検出の拡大を回避できます。

G Data マネジメントサーバー には、過去のワクチン（2種類のウイルス検索エンジン分）が保存されています。最新ワクチンで誤検出などの問題が発生した場合、問題を早急に解決するため、利用中の最新ワクチンの使用を一時的に停止し、クライアントとサブネットサーバーに過去のワクチンを配布してください。

- G Data ManagementServer に未接続のクライアント (例: 出張者が社外に持ち出したノートPC) に対しては、ロールバックは適応されません。G Data ManagementServer がクライアントに対して行ったロールバックは、クライアント側からは解除できません。

- ロールバック用に保存するワクチンの数は、**サーバー設定**で設定できます。



エンジンの種類を選択すると、**停止するバージョン**が表示されます。停止したいワクチンバージョンを選択（複数選択可）して OK を押します。これで停止したワクチンの新規配布はストップされます。また、当該ワクチンが配布済みのクライアントに対しては停止対象に設定されていないワクチンで最新のものが新たに配布されます。なお、ロールバックをクライアントに適用するには、クライアントが G Data ManagementServer と接続している必要があります。

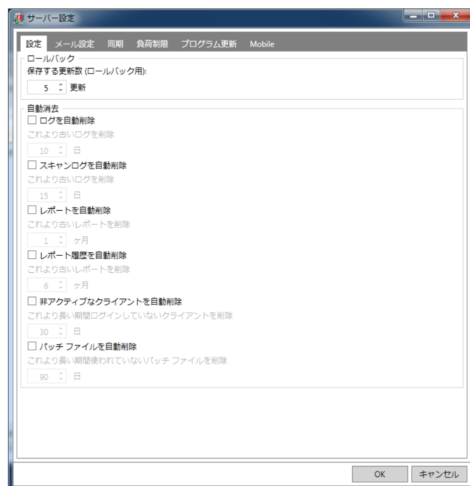
その他にも、任意の日までワクチン配布を停止する設定も可能です。この設定を行うには、**次の期限まで更新を停止** にチェックを入れ、日にちを指定してください。

サーバー設定

サーバー設定では、ManagementServer の同期、メール設定、負荷制限、段階的な配布などの設定を行うことができます。

設定

この画面では以下の設定を行うことができます。



- **ロールバック**: ロールバック用に保存するワクチンの数を入力します。デフォルトでは、5（各エンジン：5個）に設定されています。
- **自動消去**: 自動削除する頻度を項目別に設定します。
  - **ログを自動削除**: 設定日数より古いログを削除します。
  - **スキャンログを自動削除**: 設定日数より古いスキャンログを削除します。
  - **レポートを自動削除**: 設定月数より古いレポートを削除します。
  - **レポート履歴を自動削除**: 設定月数より古いレポートマネージャーのレポートを削除します。
  - **非アクティブなクライアントを自動削除**: 設定日数よりログオンしていない期間が長いクライアントを削除します。
  - **パッチファイルを自動削除**: 設定日数より長い間、利用されていないパッチファイルを削除します。

メール設定

SMTPサーバーおよび**ポート**（デフォルト: 25）には、メールサーバー名と使用するポート番号を入力します。**送信者**には、メール送信用に利用するメールアドレスを入力してください。

ここで入力したメールアドレスに、G Data セキュリティラボ からの回答が送信されます。

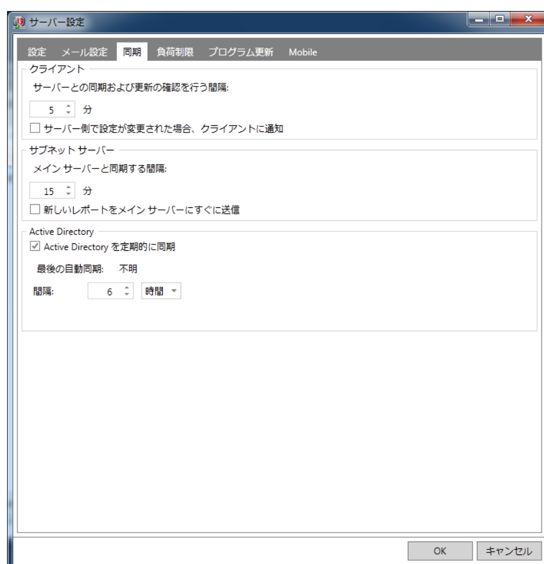
SMTPサーバーに認証が必要な場合は、**SMTP認証** ボタンから認証に関する設定を行ってください。認証方法には **SMTP AUTH** もしくは **SMTP after POP3** が選択できます。

メールグループ からは、IT管理者や経営者など自由に受信者のリストを管理できます。

同期

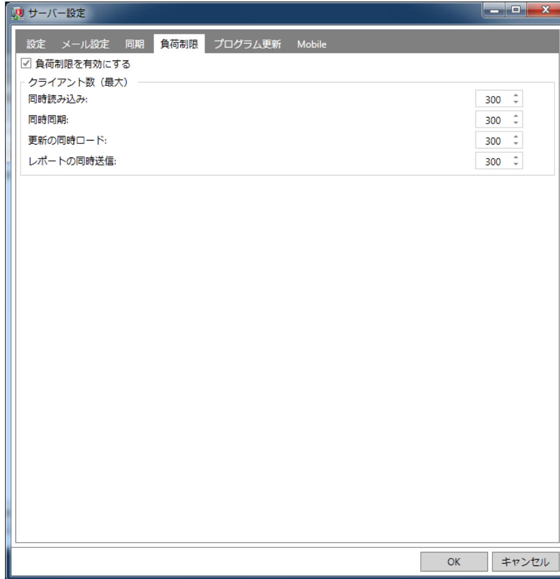
クライアント、サブネットサーバー、サーバー間の同期を実行する時間を設定します。

- **クライアント**: クライアントとサーバー間の同期間隔を指定します。**サーバー側で設定が変更された場合、クライアントに通知**にチェックを入れると、クライアントにサーバー設定の変更が行われたことを知らせる通知が送信されます。デフォルトでは、5分に設定されています。
- **サブネットサーバー**: サーバーとサブネット サーバー間の同期間隔を指定します。**新しいレポートを今すぐメイン サーバーに送信**にチェックを入れると、ここで指定した設定に依存せずに、レポートが直ちにメイン サーバーに転送されます。
- **Active Directory**: G Data ManagementServer と Active Directory の同期間隔を指定します。Active Directory との同期は、グループが Active Directory Organization Unit （組織単位）に割り当てられている場合にのみ実行されます。



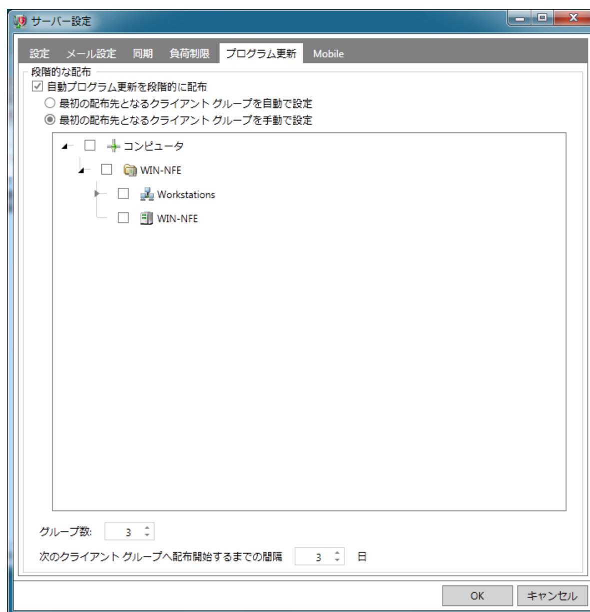
負荷制限

負荷制限を有効にするにチェックを入れると、ネットワーク内の負荷を分散させるために、一度に処理を実行するクライアントの数量を制限できます。特に、大規模ネットワークやコンピュータのスペックが低い環境では、この項目を適切に設定することによって、不要な負荷を回避できます。



プログラム更新

段階的な配布を利用すると、プログラム更新の配布を段階的に実行できます。特に大規模ネットワークでは、この機能を活用して動作テスト用マシンを指定し、更新によって問題が発生しない事を確認してからその他のクライアントにプログラム更新を配布する事をお勧めします。



段階的な配布 を有効にすると、更新を最初に受け取るグループの選択方法を、自動もしくは手動から選択できます。また、配布先グループの数やグループへの配布の時間差なども設定できます。

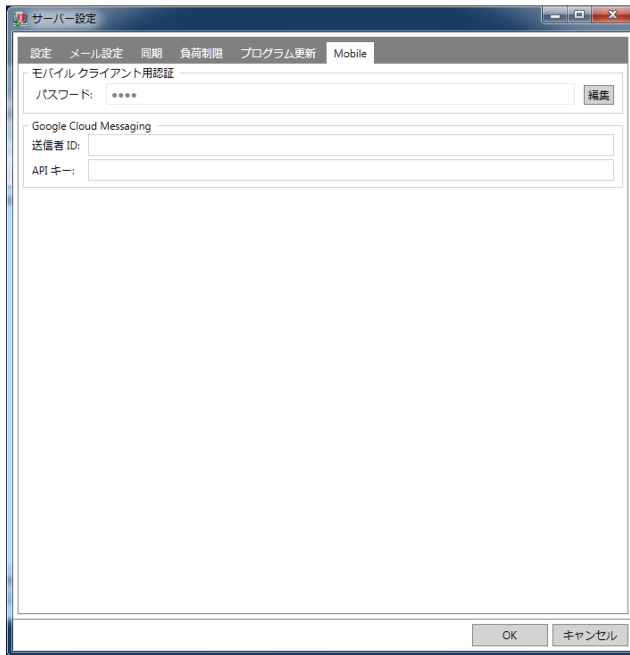
Mobile

Mobile タブでは、モバイルデバイス管理を利用するために必要な基本設定を行います。G Data Administrator 初回起動時に自動起動するサーバーセットアップ ウィザード経由で設定していなかった場合は、ここから認証用のパスワードや Google Cloud Messaging の設定ができます。

モバイル クライアント用認証には、Android 端末と ManagementServer の認証時に必要となるパスワードを設定します。モバイル設定の盗難対策機能に搭載されている、緊急時の操作を利用するためには、Google Cloud Messaging の**送信者 ID** および **API キー** が必要です。

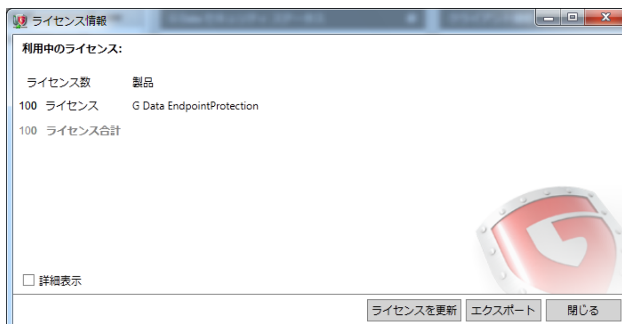
Google Cloud Messaging のプッシュ通知フレームワーク用アカウントは、Google アカウントを使って無料登録（リンク: code.google.com/apis/console）することで利用できます。まずは、Googleアカウントでログインして上記のリンクに移動します。次に、CREATE PROJECT をクリックして新規 API projectを作成してくださ

い。その後、メニューの SERVICES で GOOGLE CLOUD MESSAGING FOR ANDROID を ON にします。そして、メニューバーの API ACCESS をクリックして API　Access ページへと移動します。最後に、CREATE NEW SERVER KEY をクリックしてサーバーのIPアドレスを指定すると、API キーを生成できます。



ライセンス管理

ライセンス管理では、ご利用中の製品とライセンスに関する状況を確認できます。製品の切り替えや保護するPCの数を増やしたい場合は、本製品をお買い上げいただいた販売代理店へお問い合わせください。



［**エクスポート**］ ボタンを使うと、リストをテキストファイルにエクスポートできます。**詳細表示**にチェックを入れると、ライセンスに関するより詳細な情報を確認することができます。

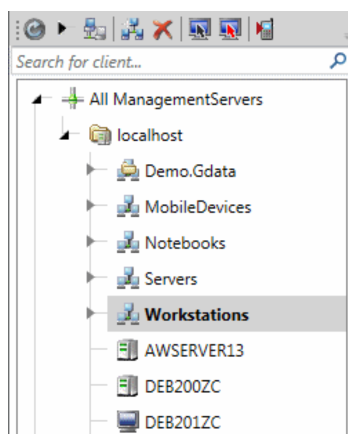
？（ヘルプ）

本製品に関する情報やオンラインヘルプを参照できます。

クライアント管理

G Data Administrator でクライアントを管理するためには、クライアント管理領域にクライアントを追加する必要があります。

クライアントを追加する場合、ネットワークの大きさや構成によって、いくつかの方法を選択する事ができます。
例えば、小さなネットワークでは、**サーバー セットアップウィザード** を使用する事でほとんどのクライアントを追加する事ができ、大きなネットワークでは、**コンピュータを検索** 機能や Active Directory エントリの割り当てを行う事で、スムーズにクライアントを追加する事ができます。



ネットワーク内の全クライアント、サーバー、およびグループはクライアント管理領域に表示されます。表示方式は、Windows Explorer のようにツリー構造の表示で、グループアイコンには小さな＋アイコンが一緒に表示されます。グループを展開する場合は、このアイコンをクリックする事でグループ内に含まれるクライアント一覧を確認できます。一方、－アイコンをクリックすると、展開しているグループを閉じます。選択したクライアントの種類によって、異なるモジュールとオプションが利用できます。例えば、PCでは **クライアント設定** タブが表示されますが、一方モバイルクライアントでは **モバイル設定** タブが表示されます。

クライアント管理領域では、個別のクライアントやグループの設定をインポート、エクスポートする事ができます。対象クライアントもしくはグループを右クリックし、**設定をエクスポート**を選択すると、**クライアント設定** と **ポリシーマネージャー**（EndpointProtection のみ搭載）の設定を .dbdat 形式で書き出すされます。**設定をインポート**を選択した場合は、その設定ファイルを読み込むことができます

<u>アイコンとツールバー</u>

クライアント管理領域では、以下のアイコンが表示されます。

 **ネットワーク**

 **サーバー**

 **サブネットサーバー**

 **グループ**

 **グループ (Active Directory リンク)**

 **クライアント**

 **Linux クライアント**

 **ノートPC クライアント**

 **モバイルクライアント**

 **Linux サーバー**

 **選択できないデバイス**: ネットワークプリンタのようなデバイスはこのアイコンで表示されます。

ツールバーでは、**組織** メニューの最も重要なコマンドがアイコンとして表示されています。利用可能なアイコンは以下のとおりです。

 **更新**

 **すべてを展開/閉じる**: ネットワークツリーの項目を展開、または折りたたみます。

 **無効なクライアントを表示**

 **新規グループを作成**

 **削除**: 一覧から対象を選択して ［**削除**］ボタンを押すと、削除できます。ここで削除したからといって、対象クライアントから G Data Security Client がアンインストールされるという事ではありません。

 **クライアントを有効化**: 対象クライアントを有効にします。

 **インストール概要**

 **インストール用リンクをモバイルクライアントに送信**: G Data Internet Security for Android のダウンロードリンクが含まれたメールをモバイルクライアントに送信します。モバイル端末のユーザーは、このリンクから G Data Internet Security for Android のインストールを開始できます。

Active Directory

G Data Administrator は、ドメインのOrganization Unit （組織単位）上の全コンピュータオブジェクトのインポートをサポートします。このためには、まず別々のグループをセットアップする必要があります。

新規作成したグループの上で右クリックすると、**Active Directory のエントリをグループに割り当て** オプションが表示されます。このダイアログで、**Active Directory のグループに割り当て** を選択し、LDAP server を選択してください。

［**選択**］ ボタンからは、利用可能なサーバー一覧を確認できます。［**追加**］ ボタンをクリックすると、別ドメインに接続することも可能です。**有効にしたコンピュータに G Data Security Client を自動的にインストール** オプションを有効にすると、Active Directory ドメインに新たに加えられてたクライアント（対象クライアントがリモートインストールの要件に合う場合） に G Data Security Client をすぐインストールします。

G Data ManagementServer は、Active Directory と60秒毎（デフォルト設定）にデータステータスを比較します。この設定値は、**サーバー設定** > **同期** から変更することができます。

組織

クライアントの管理は、インターフェース左側のツリー構造型クライアント管理領域で行います。オプションは、**組織**メニュー経由で行います。

更新

クライアント管理領域で表示されているクライアントリストの表示結果を**更新**します。

無効なクライアントを表示

このオプションを使用すると、無効になっているクライアントを表示できます。



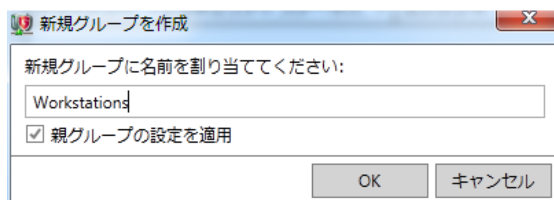
無効なクライアント
グレーのアイコンで表示されます。無効なクライアントを有効にするには、このアイコンをクリックして有効にできます。



有効なクライアント
色付きアイコンで表示されます。

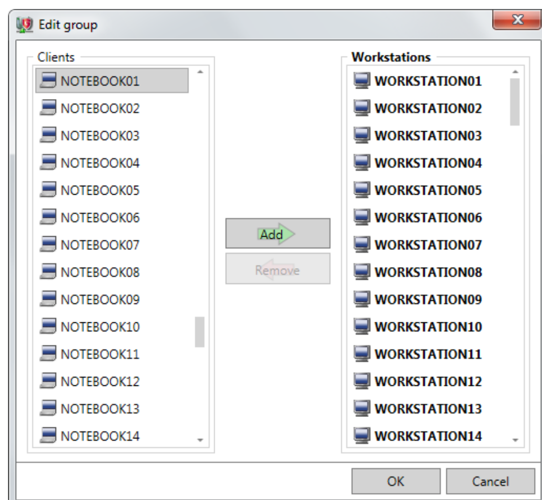
新規グループを作成

グループを作成することで、クライアント管理がより簡単になります。グループを新規作成するには、このオプションを選択して名前を入力してください。特定のクライアントをドラッグ＆ドロップでグループにまとめたり、グループ内の対象クライアントの設定を一括で処理できるようになります。



グループを編集

[追加] と **[削除]** のボタンを用いて、クライアントをグループへ割り当てたり、取り除きます。クライアント選択領域でグループを選択していない場合、この機能は選択できません。



削除

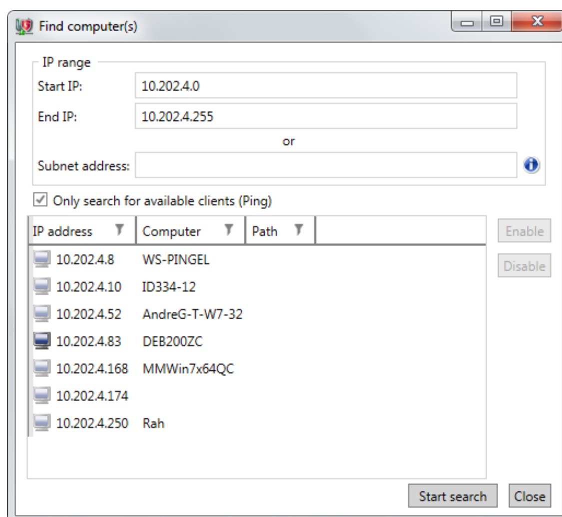
クライアント一覧からコンピュータを**削除**(＝無効化)できます。削除するには、コンピュータを選択し、クライアントメニューから**削除**を選択します。なお、コンピュータを無効にしても、クライアントにインストール済みのクライアントソフト（G Data Security Client）はアンインストールされません。

グループを削除するには、まずグループ内を空（クライアントをすべて無効にするか、別のグループに移動）にしてください。

コンピュータを検索

コンピュータを検索のウィンドウでは、クライアントを IP アドレスで検索し、G Data Administrator 上のクライアント管理領域に追加して有効化することができます。

コンピュータを検索のウィンドウでは、指定した IP アドレス範囲内のすべてのコンピュータをチェックします。この領域は、**IPアドレス（開始）** と **IPアドレス（終了）** (例: 開始に 192.168.0.1、終了に 192.168.0.255 のように入力)、もしくは **サブネットアドレス** (CIDR 表記、例: 192.168.0.0/24) のように記入します。利用可能なクライアントのみを検索するには、**アクセス可能なコンピュータのみを検索する (Ping)** を選択してください。**検索開始** を押すと、検索が開始され、検出されたコンピュータから表示されていきます。検索処理に時間がかかりすぎる場合など、処理を途中でキャンセルしたい場合は、**検索をキャンセル** を押してください。



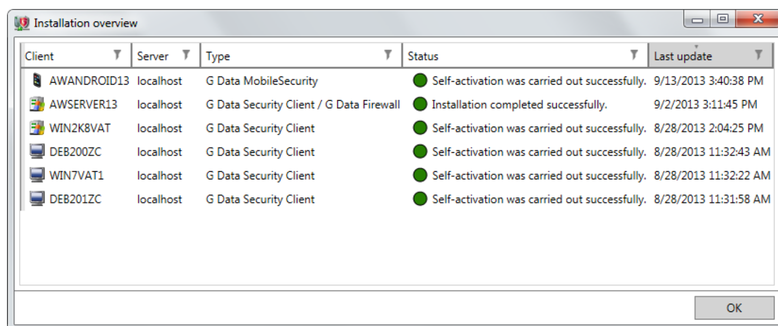
IP アドレスを使って検索したすべてのコンピュータが、IP アドレスとコンピュータ名と一緒に表示されます。**有効にする** ボタンを押すと、クライアント管理領域に表示されるようになります。検索結果には、有効化済みクライアントも表示されます。有効化済みのクライアントを無効化するには、選択してから **クライアントを無効にする** を押してください。

G Data Security Client のインストールパック を作成

G Data Security Client をサイレントインストールする実行ファイル（**GDClientPck.exe**）を作成します。インストールパックは、クライアントへのコピー、ネットワークシェア、ログインスクリプト経由でドメイン内のコンピュータに配布する、といった方法で利用すると便利です。ローカルインストールについては、**こちら**をご確認ください。

インストール概要

インストール状況を確認するには、インストール概要ウィンドウを使用します。この画面は、リモートインストールタスクが追加された場合、もしくはクライアント管理領域のツールバーのインストール概要ボタンをクリックすることで開くことができます。



インストール概要ウィンドウでは、実行済みだけでなく実行中タスクも含めたすべてのリモートインストール タスクが表示されます。**種類** のカラムには、インストールの種類 (G Data Security Client / G Data Firewall / Subnet server) が表示されます。リモートインストールが完了した後は、**ステータス** カラムで表示が更新されます。

多くの場合、リモートインストールの処理完了後は、クライアント側で再起動が必要になることがあります。再起動が必要な場合は、 **レポート** モジュール上にレポートとして表示されます。

G Data Administrator の構成

ネットワークおよびネットワーク内クライアントのセキュリティ設定とエンタープライズポリシーは、タブから選択できる様々なモジュールを通して設定できます。各モジュールの設定は、クライアント管理領域で選択しているクライアントもしくはグループに対して適用されます。それぞれのモジュールについては、各項にて解説していきます。

ほとんどのモジュールにおいて、レイアウトとリスト内のコンテンツを管理する一般オプションがあります。例えば、ページ上の表示アイテム数を減らすには、スクリーン右下の **ページあたりの数** 欄に設定された数をより少なくしてください。テキストフィルタリングを行うには、カラムヘッダーのフィルタアイコンのいずれかをクリックし、フィルタの条件を入力してください。その他のアイテムのフィルタ方法は、グループを使用する方法です。カラムヘッダーをバー上にドラッグし、カラムベースのグループを作成できます。このグループはネストして様々な表示方法に変更する事ができます。

Grouped by: G Data Security Client version ▸ Last access

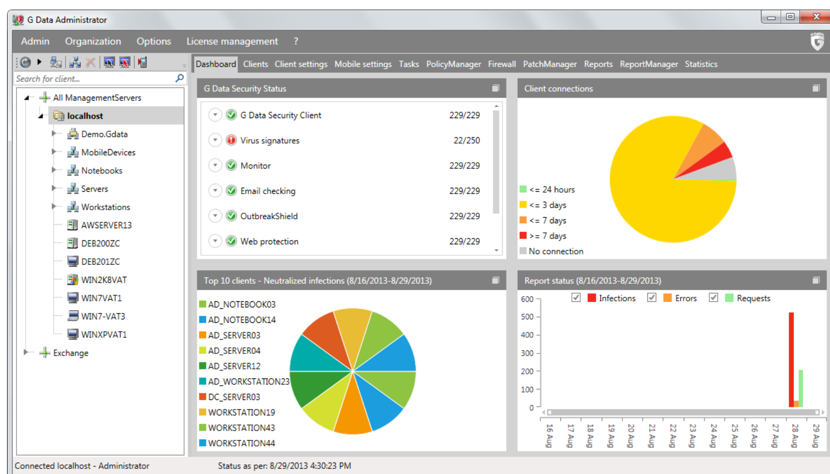
Client	Engine A	Engine B	Last access
G Data Security Client version: (21)			
G Data Security Client version: 12.0.0.222 (11.01.2013) (1)			
G Data Security Client version: 12.0.0.239 (11.04.2013) (28)			
G Data Security Client version: 13.0.0.13 (29.08.2013) (1)			
G Data Security Client version: 13.0.0.7 (25.08.2013) (197)			
Last access: (11)			
Last access: 8/21/2013 1:53:53 PM (5)			
Last access: 8/25/2013 1:53:53 PM (6)			
Last access: 8/26/2013 1:48:01 PM (7)			
AD_NOTEBOOK14	AVA 22.12133 (28.08.2013)	AVL 22.1928 (28.08.2013	8/26/2013 1:48:01 PM
AD_NOTEBOOK15	AVA 22.12133 (28.08.2013)	AVL 22.1928 (28.08.2013	8/26/2013 1:48:01 PM
AD_NOTEBOOK16	AVA 22.12133 (28.08.2013)	AVL 22.1928 (28.08.2013	8/26/2013 1:48:01 PM
AD_NOTEBOOK17	AVA 22.12133 (28.08.2013)	AVL 22.1928 (28.08.2013	8/26/2013 1:48:01 PM

各モジュールの設定を変更した場合は、**適用**をクリックするとその設定がクライアントへ転送され、**キャンセル**をクリックすると変更した設定は転送されず破棄されます。グループ内に複数の設定が存在する場合、それらの設定は未定義のステータスとして表示され、新しく設定を適用するまで保存されません。

多くのモジュールの画面下部には**情報**欄があり、設定の適用状況に関するステータスを確認できます。

ダッシュボード

ダッシュボードでは、ネットワーク内のクライアントに関する最新情報が表示されます。



G Data セキュリティ ステータス

クライアント管理領域で選択したクライアントもしくはグループに関するセキュリティ設定の確認や操作を行います。



対象は安全な状態にあります。
対象は適切に保護されている場合、この緑色のアイコンが表示されます。



対象は注意が必要な状態にあります。
ウイルスガードが無効、使用しているワクチンが古い場合などに、このアイコンが表示されます。



G Data Administrator の起動直後は、ほとんどの項目でこのアイコンが表示されることがあります。これは、G Data ManagementServer と G Data Administrator 間で実行される保護ステータス確認が処理中のため、このように表示されます。赤いアイコンが表示されている間も、コンピュータは保護されていますので、ご安心ください。

ステータスが表示されている項目をダブルクリックすると、操作実行や各機能の画面へ移動します。赤いアイコンが表示された項目で最適な操作を行うと、ステータス領域のアイコンは再び緑に切り替わります。

クライアント接続

各クライアントPC（もしくはグループ）とG Data ManagementServer 間の接続に関する情報を表示します。

保護したクライアント トップ 10

このリストに表示されるクライアントに対しては、得に注意を払う必要があります。クライアントユーザーへ通知し、感染回避のための対策を講じることをお勧めします。ユーザーの利用方法に問題があり、インターネットやデバイスの使用制限で感染を回避できそうな場合は、**ポリシーマネージャー**（G Data EndpointProtection Businessのみ）で当該ユーザーの権利を制限することをお勧めします。

レポートステータス

特定期間内にネットワークで発生した感染数、要求、エラーなどをグラフで表示します。

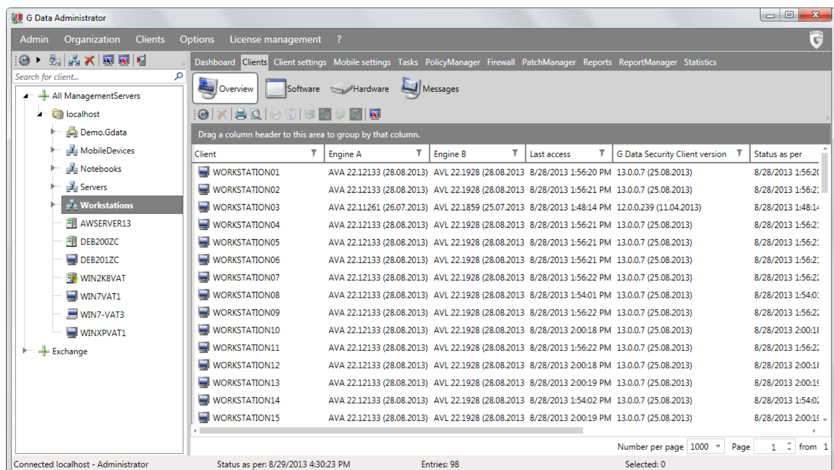
クライアント

クライアント管理領域でグループを選択すると、そのグループに属するクライアントが一覧表示されます。また、クライアントに関しては、インストールされているプログラムのバージョン情報、ワクチンのバージョン情報、最後にG Data マネジメントサーバーに接続した日時などの情報が一覧でき、クライアントの稼動状態を確認できます。

タブ上部にある**一覧**アイコンでは、クライアントの**一覧**情報を確認できます。その隣の**メッセージ**アイコンからは、個々のクライアントにメッセージをを送付することができます。このメッセージによって、ユーザーは迅速かつ簡単にクライアントステータスの変化を把握できます。また、クライアントモジュールでは、クライアントの**ハードウェア**および**ソフトウェア**に関する情報を一覧表示することができます。

一覧

一覧では、クライアント管理領域で指定したクライアントに関する情報が表示され、ここから操作を直接実行できます。表示する内容は、カラムをクリックすることでフィルタや並べ替えができます。並び替えを適用中のカラムには小さな矢印が表示されます。



カラムヘッダー上で右クリックして、**表示するカラムを選択** を選択すると、クライアント一覧で表示させる以下のプロパティ項目を選択できます。

- サーバー
- Alias（サーバー）
- クライアント
- エンジン A
- エンジン B
- データステータス
- G Data Security Client のバージョン
- 言語
- UPMS クライアント
- 最終アクセス
- ワクチン更新/実行日
- プログラムファイル更新/実行日
- OS
- サブネットサーバー
- ドメイン
- ネットワークカード
- MAC アドレス
- IPv4 アドレス
- IPv6 アドレス
- サブネットマスク
- デフォルト ゲートウェイ
- DNS サーバー
- DHCP サーバー
- Primary WINS
- Secondary WINS
- EULA

クライアントを管理するには、リスト上のツールバーから以下のオプションを使うことができます。

 **更新**: 表示を最新状態に更新します。

 **削除**: クライアントビューからクライアントを取り除きます。

 **印刷**: クライアントのリストを印刷します。選択画面では、印刷対象を指定することができます。

 **ページレイアウト**: プリントするページのプレビュー表示します。

 **G Data Security Client をインストール**

 **G Data Security Client をアンインストール**

 **今すぐワクチンを更新**: クライアントのワクチンを更新し、G Data ManagementServer から最新ワクチンをロードします。

 **ワクチンを自動更新**: ワクチンの自動更新を有効にします。クライアントは、定期的に G Data ManagementServer 上に最新ワクチンがないかチェックし、新しいワクチンが利用できる場合は、自動更新を実行します。

 **今すぐプログラムファイルを更新**: G Data ManagementServer 上に新しいプログラムファイルがある場合、プログラムファイルをロードして更新します。プログラム更新後は、クライアント側で再起動が必要になる場合があります。

 **プログラムファイルを自動更新**: プログラムファイルの自動更新を有効にします。クライアントは、定期的に G Data ManagementServer 上に最新のプログラムファイルがないかチェックし、新しいプログラムが利用できる場合は、自動更新を実行します。

 **インストール概要**

<u>メニューバー</u>

一覧タブが選択されると、メニューバー上に**クライアント**という名前の追加メニューが表示されるようになります。このメニューからは、クライアント選択して右クリックした時の操作の他、クライアントに対して様々な操作を実行することができます。.以下のオプションが含まれています。

- **G Data Security Client をインストール**
- **G Data Security Client for Linux をインストール**
- **G Data Security Client をアンインストール**
- **インストール概要**
- **デフォルト設定に戻す**: クライアント（およびグループ）のセキュリティ設定をリセットします。

- **G Data Security Client をグループに移動**: 選択したクライアントを既存のグループへ移動します。この機能を選択すると、作成済みの全グループがダイアログ内に表示されます。クライアントをグループに移動するには、グループを選択して ［OK］ をクリックします。
- **割り当てられた EULA を編集**: 選択したクライアントに割り当て済みの **EULA** を編集します (モバイル クライアントでのみ利用可)。
- **割り当てられた EULA を削除**: 割り当て済みの EULA を選択したクライアントから取り除きます (モバイル クライアントでのみ利用可)。
- **EULA 管理**
- **サブネットサーバーを割り当て**: **サーバー管理** の機能で特定サブネットサーバーへクライアントを割り当てることができますが、この機能も同じように個々のクライアントをサブネットサーバーへ割り当てることができます。
- **今すぐワクチンを更新**
- **ワクチンを自動更新**
- **今すぐプログラムファイルを更新**
- **プログラムファイルを自動更新**
- **プログラム更新後に再起動**: クライアント用プログラムファイルの更新後に行う動作を設定します。クライアントユーザーに再起動の実行を促す場合は、**クライアント側でメッセージボックスを表示** を選択してください。**レポート作成** を選択すると、 **レポート** タブ内に関連レポートが作成されます。また、**確認せずに再起動** を選択すると、クライアント側で強制的に再起動を自動実行します。

G Data Security Client をインストール

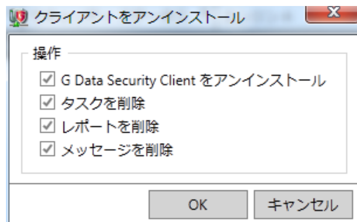
G Data Security Client のリモートインストールを実行するには、**G Data Security Client をインストール** のオプションを選択してください。

> 無効になっているクライアントにアクセスするには、まずクライアントがクライアントリスト上で有効化されている必要があります。G Data Security Client をインストールを実行した場合は、ソフトがこれを通知して、無効化されているクライアントが表示されるようになります。

リモートインストールでインストールできない場合は、製品メディアもしくはインストールパックを使ってインストールすることもできます。

G Data Security Client をアンインストール

この機能を使うと、G Data Security Client をアンインストールできます。アンインストールを実行する際は、そのクライアントに属するタスク、レポート、メッセージを G Data ManagementServer 上から削除するかどうかを選択できます。
それぞれを選択し終わった後、OKをクリックすると実際にアンインストール処理が開始されます。プログラムをクライアントから完全に削除するにはアンインストール処理が終わった後に対象クライアントの再起動が必要です。



リモートではなく、ローカルでクライアントプログラムをアンインストールすることも可能です。
これを実行するには管理者権限を持つアカウントを使って、コマンドプロンプト経由で実行する必要があります。

アンインストールを開始するには、コマンドプロンプトで

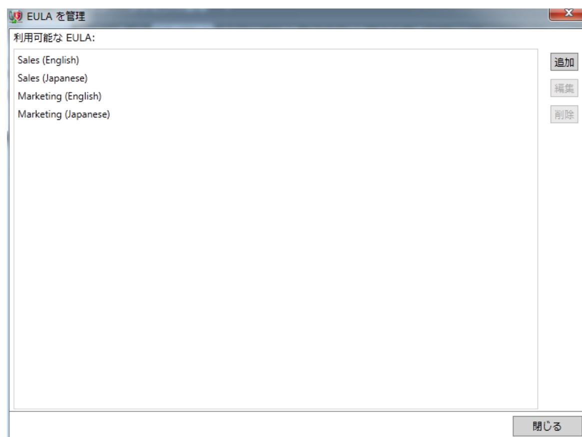
C:\Program Files (x86)\G DATA\AVKClient フォルダを指定し、コマンド *UnClient / AVKUninst* を実行してください。

このコマンドでアンインストール処理を行った後も再起動が必要です。

EULA管理

EULA管理ウィンドウでは、モバイル端末用の社内向け EULA (使用許諾契約) の追加、編集、削除ができます。

リモート管理を行っている端末に対して G Data のモバイルアプリでどのような管理を行っているか、その他の端末利用に関する規則など、管理者自身が作成した使用許諾文を設定し、アプリのセキュリティセンター画面に表示させることができます。



EULA を編集のウィンドウでは、すべての利用可能な EULA が表示されます。EULA を追加するには、**追加** を押してください。EULA ウィンドウを作成するには、**名前**を入力して**言語**を選択し、契約書の**内容**を追加してください。**OK** を押すと、EULA がリストに追加されます。

既存の EULA を編集するには、リストから対象を選択して **編集**をクリックします。EULA を削除するには、 **削除**を押してください。

ソフトウェア

ソフトウェア一覧では、ネットワーク内で利用されているソフトウェアが一覧表示されます。ソフトウェアはブラックリストまたはホワイトリストに追加でき、ソフトウェアを簡単な操作で管理できます。

ブラックリストおよびホワイトリスト上のアイテムリストは、次のツールバーボタンを使って管理できます。

 **更新**: ソフトウェア一覧を更新します。



すべて表示: クライアントにインストールされているすべてのソフトウェアを表示します。



印刷: ソフトウェア一覧を印刷します。選択画面では、印刷対象を指定することができます。



ページレイアウト: プリントするページのプレビュー表示します。



ブラックリストのソフトウェアのみ表示: ブラックリストに追加済みのソフトウェアのみ表示します。



ホワイトリストにないソフトウェアのみ表示: ネットワーククライアントにインストールされたソフトで、システム管理者によるチェックがまだ行われていないソフトウェアのみ表示します。この表示方法を使うと、対象のソフトウェア上で右クリックして簡単にブラックリストまたはホワイトリストに登録することができます。

リスト領域では、クライアント管理領域で選択したクライアント上にインストールされているソフトウェアを表示します。ソフトウェアをブラックリストもしくはホワイトリストに登録するには、［**ブラックリスト**］ または ［**ホワイトリスト**］のボタンをクリックしてください。新規ブラックリストもしくはホワイトリストを登録するには、［**追加**］ をクリックしてください。［**属性情報を取得**］からは、ブラックリストもしくはホワイトリストに登録するプログラムの属性を入力します。属性のルールを作成するには、属性のチェックボックスにチェックを入れてください。これにより、特定ベンダのプログラムやプログラムバージョンをリスト化できます。このプログラム属性をすでに知っている場合は、**属性情報を取得**ダイアログを使わなくても、直接ブラックリストもしくはホワイトリストに追加することもできます。

ハードウェア

ハードウェア一覧では、クライアント側で使用されているハードウェアに関する情報を一覧で表示します。

カラムヘッダー上で右クリックした後、**表示するカラムを選択** をクリックすると、リストビューに表示する追加カテゴリを選択できます。

ここで表示できるカテゴリは以下の通りです。

- クライアント
- CPU
- CPU クロック周波数 (MHz)
- メモリ
- 空きシステム容量
- システム容量 (統計)
- 空き容量 (合計)
- 合計容量 (統計)
- システムメーカー
- システム名
- システムバージョン
- システムファミリー
- CPU ID
- マザーボードメーカー
- マザーボード
- マザーボードバージョン
- BIOS メーカー
- BIOS 発行日
- BIOS バージョン

ハードウェア一覧は、次のツールバーボタンを使って管理できます。

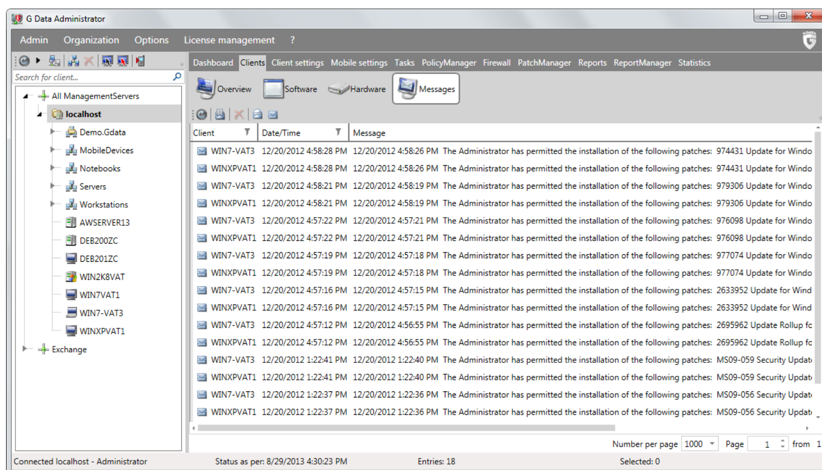
 **更新**: ハードウェア一覧を更新します。

 **印刷**: ハードウェア一覧を印刷します。選択画面では、印刷対象を指定することができます。

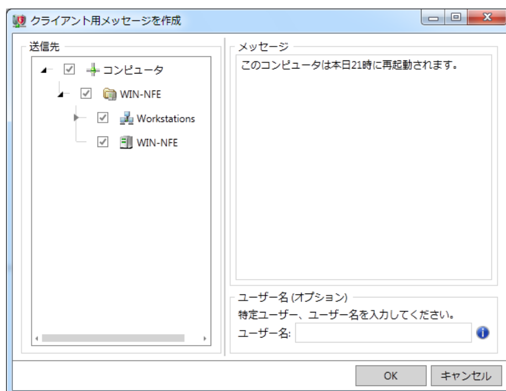
 **ページレイアウト**: プリントするページのプレビュー表示します。

メッセージ

個々のクライアントまたはクライアントグループに対してメッセージを送付し、クライアントユーザーにステータス変化について通知することができます。このメッセージはクライアントの画面右下にポップアップ表示されます。



メッセージを作成するには、［**新規メッセージ**］アイコンをクリックするか、右クリックメニューから**新規メッセージ**を選択します。します。ダイアログが開くので、メッセージ送付先のクライアントを選んでください。メッセージ送信をクライアントPCもしくはネットワーク内の特定ユーザーに限定する場合は、**ユーザー名**にログイン名を入力してください。**メッセージ**フィールドに情報を入力した後は、［OK］ボタンをクリックしてください。



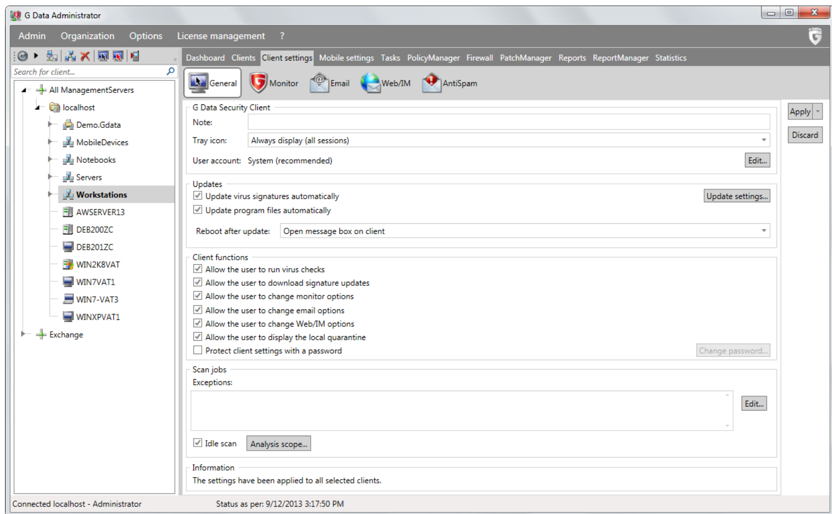
クライアント設定

クライアント設定では、個々のクライアント、またはクライアントを含むグループを対象とした設定を管理できます。一般、ウイルスガード、メール、Web/IM、およびアンチスパムから、ネットワーク内のクライアント用の保護設定をカテゴリごとに管理できます。

※アンチスパムは、G Data ClientSecurity Business / G Data EndpointProtection Business にのみ搭載されています。

一般

一般タブでは、選択したクライアントの一般的な設定を確認したり、変更できます。



G Data Security Client

G Data Security Client 領域ではクライアントの一般的な設定を行うことができます。

- **コメント**: クライアントにわかりやすい名前などをつけます。
- **タスクバーのアイコン**: ターミナルサーバーおよびWindows XP / Vista / 7 / 8 では、クライアントアイコンをタスクバー上に表示させるセッションを、**常に表示**、**最初のセッションのみ表示** (ターミナルサーバー用)、または**表示しない**の中から選択できます。クライアントPC上で、G Data Security Client の各種機能にアクセスするには、このアイコンが表示されている必要があります。

- **ユーザーアカウント**: G Data Security Client は、通常、システムアカウント上で稼動します。ネットワークディレクトリをスキャンできるようにするには、ここで別アカウントを入力してください。このアカウントにはクライアントに対する管理者権限が必要です。

更新

更新領域ではワクチンやプログラム更新に関わる設定を行うことができます。

- **ワクチンを自動更新**: ワクチンの自動更新を有効にします。自動更新を有効にすると、クライアントはG Data G Data ManagementServer に定期的に新しい更新があるか確認し、更新が利用できる場合は、自動更新します。

- **プログラムファイルを自動更新**: G Data ManagementServer 経由でクライアントのプログラムファイルを自動更新します。プログラムファイルの更新後は、クライアントの再起動が必要になる場合があります。再起動に関わる動作の設定は、**更新後に再起動**で設定します。
- **更新後に再起動**: [**クライアント側でメッセージボックスを開く**] を選択すると、今すぐ再起動もしくは後で再起動するかをユーザーに選択させることができます。[**レポート作成**] では、G Data Administrator の **レポート** タブ内にレポートを作成します。プログラムファイル更新後にクライアントPCを強制的に再起動させるには、[**確認せずに再起動**] を選んでください。
- **更新設定**: クライアントがワクチン更新を行う際の経路を設定します。G Data ManagementServer 経由のダウンロード以外にも、クライアントがインターネット接続経由で直接ワクチン更新を取得する設定も可能です。 ノートPCなどにお勧めの設定として、クライアントが G Data ManagementServer と接続できる場合は ManagementServer 経由で更新をロードし、ManagementServer と接続できない場合は、インターネット経由でワクチン更新を実行する設定もあります。**設定とスケジュール** ボタンを押すと、ManagementSetverに接続していない場合のワクチンのダウンロード間隔を設定できます。

クライアント側の機能

この領域ではクライアントに対して付与する操作権限の設定を行うことができます。社内のセキュリティーポリシーやネットワークポリシーなどに応じて、権限の度合いを調整してください。

- **ユーザーによるウイルススキャンの実行を許可**: クライアントユーザーが任意でウイルススキャンを実行できるようになります。スキャンの結果は、クライアントが次回 G Data ManagementServer と通信する際に送信されます。
- **ユーザーによるワクチン更新のダウンロードを許可**: クライアントPCのユーザーが、G Data ManagementServer を経由せず、インターネットから直接更新できるようになります（推奨： 社内ネットワークの外で利用されているクライアントPC）。
- **ユーザーによるウイルスガードオプションの変更を許可**: クライアントPCのユーザーが **ウイルスガード** のオプションを設定できるようになります。

- **ユーザーによるメールオプションの変更を許可**: クライアントPCのユーザーが **メール保護、アンチスパム** ※のオプションを設定できるようになります。
  ※アンチスパムは、G Data ClientSecurity Business / G Data EndpointProtection Business にのみ搭載されています。
- **ユーザーによるWeb/IMオプションの変更を許可**: クライアントPCのユーザーが **Web/IM** のオプションを設定できるようになります。
- **ローカルの隔離領域を表示**: ウイルスガードが隔離したファイルをクライアントユーザーが操作（駆除、削除、元に戻す）できるようになります。この設定は、コンピュータに関して一定の知識を有するユーザーにのみ許可してください。
- **オプション変更をパスワードで保護**: クライアントユーザーによる不適切な設定変更を防ぐため、オプション変更をパスワードで保護します。パスワードは、クライアントまたはグループ単位で割り当てることができます。

スキャンジョブ

この領域では、スキャンジョブの実行時にスキャン対象から除外する例外ディレクトリを指定できます。アーカイブおよび復元用パーティションなど、スキャンジョブの例外フォルダとして定義できます。また、ファイル拡張子も例外として設定できます。例外ディレクトリは、グループ全体に対しても定義できます。グループ内のクライアントにすでに例外ディレクトリが定義されている場合も、新規ディレクトリを追加したり、既存ディレクトリを削除したりできます。その際、個々のクライアントの例外ディレクトリの定義は引き続き保持されます。ウイルスガードの例外についても、同様に扱われます。

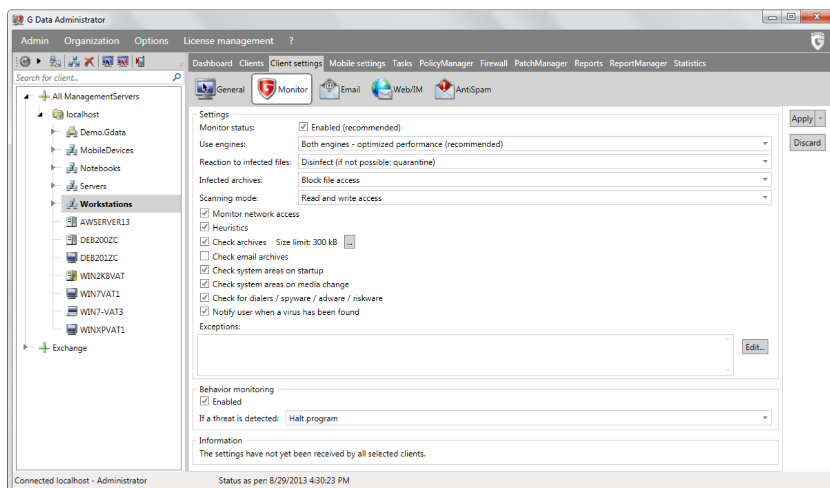
アイドリングスキャンにチェックを入れるとクライアントPCのアイドル状態中にスキャンを実行させることができます。［**スキャン範囲**］をクリックすると、アイドリングスキャン中にスキャンを行う範囲（デフォルト: すべてのローカルハードドライブ）を設定できます。

> **Linux ファイルサーバーのスキャンジョブにおける留意点：**
> ディレクトリの選択では、ルートドライブ ("/") およびすべての共有ディレクトリが表示されます。

ウイルスガード

選択した対象クライアントまたはグループに対して、ウイルスガードの設定を行います。変更した設定は、**[適用]** をクリックして変更を保存した後に、適用されます。**[キャンセル]** をクリックすると、G Data ManagementServer の設定は、以前の設定が引き続き適用されます。グループ内のクライアントがあるオプションに関して異なる設定がなされている場合は、未定義ステータスとして割り当てられます。未定義の設定値は、適用しても保存されません。

ウイルスガードは本製品において非常に重要な機能です。この機能を無効にすると、コンピュータをマルウェアからリアルタイムで保護できなくなります。特殊なケースを除き、ウイルスガードは無効にしないでください。ウイルスガードは例外設定が可能です。ウイルスガードが特定アプリケーションの起動速度に影響を及ぼしている場合は、関連のプログラムファイル、プロセス、ファイルなどを例外として設定します。なお、ウイルスガードから除外するファイルは、その安全性を確かめた上で、例外として登録してください。



設定

Monitor settings ウイルスガードの設定領域では、スキャンの設定変更や例外設定を行う事ができます。

- **ウイルスガードのステータス**: ウイルスガードのオン/オフを切り替えます。最適なウイルス保護を実現するためにも、通常は、常にオンの状態でご利用ください。

- **エンジンの種類**: G Data は、2種類のウイルス検索エンジンを搭載し、最適なウイルス保護を実現しています。通常は、2つのエンジン （**検出: 最高レベル/パフォーマンス:最適 推奨**）を選択してください。1種類のエンジンだけでの稼動も可能ですが、ウイルス保護性能が若干落ちます。1種類のエンジンは、コンピュータのパフォーマンスに問題がある場合にのみ、ご使用ください。

- **感染した場合**: ファイルにウイルス感染検出された場合の対処方法を指定します。使用環境や使用マシンに適した対処方法を選択してください。
  - **ファイルアクセスをブロック**: 感染ファイルへの読み込み/書き込みができないように、ファイルアクセスをブロックします。

 - **ウイルス駆除 (不可能な場合: ファイルアクセスをブロック)**: ウイルスを駆除します。駆除できない場合は、感染ファイルへのファイルアクセスをブロックします。
 - **ウイルス駆除 (不可能な場合は隔離)**: ウイルスを駆除します。駆除できない場合は、感染ファイルを隔離領域に移動します。
 - **ウイルス駆除 (不可能な場合はファイルを削除)**: ウイルスを駆除します。駆除できない場合は、ファイルを削除します。ファイルを削除すると、大量のデータを消失したり、システムに問題を及ぼす可能性もあります。実行時には十分にご注意ください。
 - **ファイルを隔離**: 感染ファイルを隔離領域に移動します。駆除が可能な場合は、G Data Administrator から操作します。
 - **削除**: 感染ファイルを削除します。この操作を実行すると、大量のデータを消失したり、システムに問題を及ぼす可能性もあります。実行時には十分にご注意ください。

- **感染したアーカイブ**: アーカイブからウイルスを検出した場合、ファイルからウイルスを検出時とは別の処理方法で対応できます。通常、アーカイブに格納されたウイルスは、アーカイブを解凍しなければ活動を開始しません。

- **スキャンモード**: ウイルスガードの実行タイミングを設定します。設定は、読み取り/書き込み時にスキャン、読み取り時にスキャン、実行時にスキャンから選択できます。

- **ネットワークアクセスをスキャン**: ネットワークアクセスに関するウイルスガードの処理操作を定義します。ネットワーク全体を G Data で監視している環境では、ネットワークアクセスのスキャンは適用されません。

- **ヒューリスティック**: ヒューリスティック検出で、ウイルスが持つ特徴に基づいて未知ウイルスを検出します。

- **アーカイブ**: アーカイブ内の圧縮ファイルのスキャンには、非常に多くの時間が掛かるため、通常は容量制限をかけるか無効にしておくことをお勧めします。この機能を無効にしても、ウイルスが含まれている場合は、ファイルを解凍する際にウイルスガードが検知・ブロックします。アーカイブスキャンの実行をアーカイブサイズで制限するには、[...] から設定します。

- **メールアーカイブをスキャン**: メールアーカイブをスキャンします。スキャンには非常に多くの時間が掛かるので、この機能は通常は無効にしておくことをお勧めします。この機能を無効にしても、メールの添付ファイルにウイルスが含まれている場合は、ウイルスガードが検知・ブロックします。Microsoft Outlook では専用プラグインで送受信メールを保護します。

- **起動時/メディア交換時にシステム領域をスキャン**: システム領域（例: ブートセクター）のスキャンは非常に重要です。この機能もしくはメディア交換時にシステム領域をスキャンのうち、いずれかは必ず有効にしてください。

- **ダイヤラ / スパイウェア / アドウェア / リスクウェアをスキャン**: ダイヤラ、スパイウェア、アドウェア、キーロガーなど、ユーザーに様々な損害を与える危険性のある不正プログラムをスキャンします。これらの不正プログラムは、ユーザーの気づかないところで、高額な接続先に接続したり、ユーザーのインターネット閲覧履歴やパスワードやキーストロークを記録し、その情報を第三者に送信します。

- **ウイルス検出時にユーザーに通知**: ウイルス検出時に、クライアント上でメッセージを表示してクライアントユーザーに検出を通知します。

例外領域で**編集**をクリックすると、クライアント上の特定ディレクトリや特定種類のファイルだけをスキャンするように設定できます。普段使用しないアーカイブのスキャンなどを省略して、スキャン時間を削減できます。

- **ドライブ**: ディレクトリのボタンをクリックし、ドライブ（パーティション、ハードディスク）を選択します。
- **ディレクトリ**: ディレクトリのボタンをクリックし、フォルダ（サブフォルダも含む）を選択します。
- **ファイル**: 例外設定するファイル名を指定します。ファイル名には特殊文字（ワイルドカード）を利用できます。
- **プロセス**: 特定プロセスをウイルスガードの監視から除外するには、ここで対象のディレクトリやプロセス(例 *C:|Windows|system32|cmd.exe*)を指定します。

ここで設定した例外設定は、**ウイルスガードの例外**からいつでも編集や削除ができます。

特殊文字（ワイルドカード）機能について

例外指定には以下のワイルドカードが利用できます。

- **クエスチョンマーク** (?) には、個々の文字が当てはめられます。
- **アスタリスク** (*) には、文字列が当てはめられます。

例: exe拡張子ファイルをすべて例外指定するには、***.exe** と入力します。異なる表計算フォーマット（例： xlr、 xls）を指定するには、***.xl?** と入力します。また、ファイル名は同じでも種類の異なるファイルを指定するには、**text*.*** と入力します。

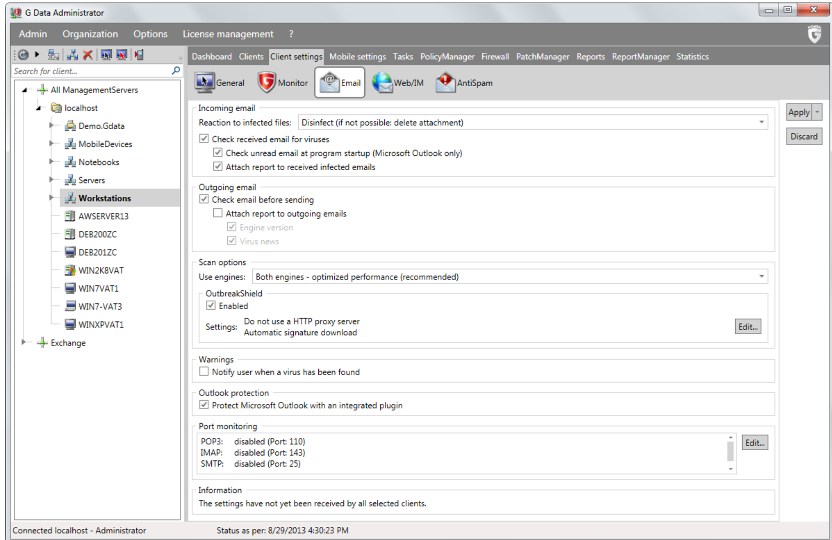
ふるまい検知（ビヘイビアブロッキング）

ふるまい検知（ビヘイビアブロッキング）はウイルスガードとは独立した保護機能です。ウイルスガードとは異なり、定義ファイルベースではなくプログラムの様々なふるまい、例えばレジストリやオートスタートエントリを分析し、不審なプログラムを検出します。

ふるまい検知を有効にするには、有効にチェックを入れ、**脅威が検出された場合**で不正プログラムが検出された際の処理方法を、**ログを残すのみ**、**プログラムを停止** 、**プログラムを停止して隔離**から選択してください。

メール

G Data Security Client がインストールされたクライアントPCに対し、メール保護を設定します。メール保護では、**POP3**、**IMAP**、**SMTP** プロトコルをチェックします。また、**Microsoft Outlook** には、専用プラグインが用意されており、すべての送受信メールでウイルススキャンを実行します。



受信メール

受信メール領域では、受信メールのスキャンに関する設定を行う事ができます。

- **感染した場合**: 感染ファイル検出時の処理操作を指定します。処理操作は使用環境に応じて、適切な設定を選択してください。

- **受信メールをスキャン**: クライアントの受信メールをすべてスキャンします。
- **起動時に未読メールをスキャン (Microsoft Outlook のみ)**: Microsoft Outlook の起動時に、受信ボックス内の未読メールをすべてスキャンします。
- **ウイルス感染の受信メールにレポートを添付**: クライアントへの送信メールにウイルスが混入している場合は、メール本文に「**注意! このメールには次のウイルスが含まれています。<ウイルス名>**」、メールの件名の前に「**ウイルス**」と警告メッセージを挿入します。**添付ファイル/本文を削除** のオプションを有効にすると、メールの感染部分が削除されたことが通知されます。

送信メール

送信メール領域では、送信メールのスキャンに関する設定を行う事ができます。

- **送信前にメールをチェック**: ウイルス感染メールの送信を防ぐため、送信前にチェックすることができます。メールにウイルスが含まれる場合、 *このメール [件名] には次のウイルスが含まれています: [ウイルス名]* というメッセージが追加され、メールは送信されません。
- **送信メールにレポートを添付**: このオプションを有効にすると、送信メール本文の末尾に以下のようなレポートを表示できるように設定できます（**ワクチンバージョン**と**ウイルスニュース**は、表示/非表示を指定可）。このオプションは**送信前にメールをチェック**を有効にすると選択できます。

例	G Data AntiVirus によってウイルススキャンされています。 バージョン： GDAV 19.0.37 （01.10.2011） ウイルス情報： www.antiviruslab.com

スキャンオプション

スキャンオプション領域では、受信/送信メールのスキャンに関する詳細設定を行う事ができます。

- **エンジンの種類**: G Data は、2種類のウイルス検索エンジンを搭載し、最適なウイルス保護を実現しています。通常は、**2つのエンジン （推奨）**を選択してください。1種類のエンジンだけでの稼動も可能ですが、ウイルス保護性能が若干落ちます。1種類のエンジンは、コンピュータのパフォーマンスに問題がある場合にのみ、ご使用ください。

- **アウトブレイクシールド**: アウトブレイクシールドは、インターネット上の大量のスパムメールやウイルスの発生を常時監視するクラウド型サービスです。新種ウイルスが発生しても、ウイルスに対するワクチンが提供されるまでの間、最新のウイルスをほぼリアルタイムで検出して無害化し、ワクチン生成までのタイムラグを埋めてシステムの安全性を確保します。アウトブレイクシールドを利用するにはインターネット接続が必要です。**[編集]** からは、アウトブレイクシールドの能力を更に高める事ができる追加定義ファイルのダウンロード間隔や、接続用のプロキシに関する情報を設定できます。

警告メッセージ

警告メッセージ領域では、感染メールを受信した際の通知に関する設定を行う事ができます。

- **ウイルス検出時にユーザーに通知する**: 感染メールの受信をメール受信者に通知できます。受信者の画面には警告メッセージが表示されます。

Outlook 保護

Microsoft Outlook は専用プラグインによりメールをスキャンする事ができます。

- **専用プラグインで保護**: この機能を有効にすると **Microsoft Outlook** 用のプラグインが有効になり、このプラグインによる送受信メールのスキャンが行われるようになります。また、**ツール**メニューに**フォルダ内のウイルスをスキャン**の機能が追加されます。この機能では、G Data Administrator に依存することなく、クライアント側で選択したメールフォルダをスキャンすることができます。メールの添付ファイルをスキャンするには、メール画面のメニューバーから [**ツール**] > [**メールをウイルススキャン**] を選択します。スキャン完了後は、分析結果が表示されます。

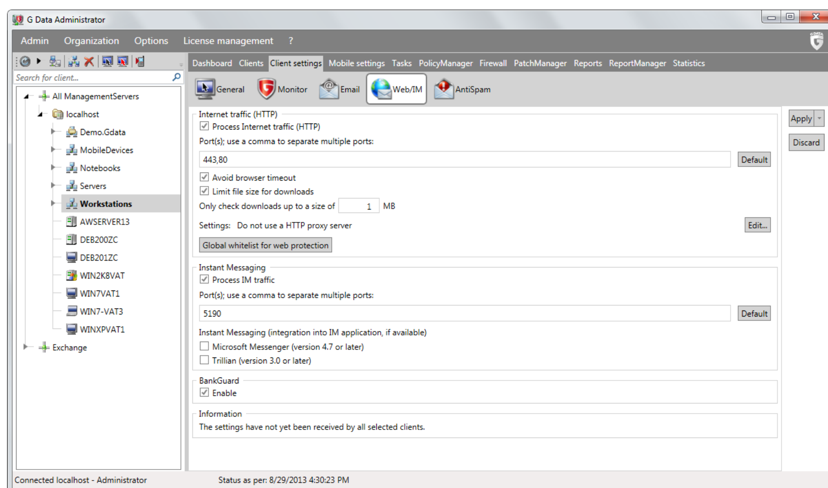
※Outlook 専用プラグインの使用中にメール送受信の問題が出る場合は、専用プラグイン、もしくは**ポート監視**によるメールスキャン、いずれかを停止してください。その場合でも、有効になっている機能でメールスキャンは行われます。

ポート監視

デフォルト設定では、POP3 (110)、IMAP (143)、SMTP (25) の標準ポートをスキャン用に監視します。システムのポート設定がこれらのポートを使用していない環境では、[**編集**] から設定変更を行い対応したポートに変更してください。

Web/IM

Web/IMでは、インターネットトラフィック、インスタントメッセンジャー、ネットバンキングなどに関するスキャン設定を行います。パフォーマンスに関する問題でインターネットコンテンツをオフにする場合、ウイルスガードを必ずオンにしておいてください。ウイルスガードは、ユーザーがインターネットコンテンツのチェック機能でスキャンされず、コンピュータにダウンロードされた感染ファイルへアクセスする時に検出を行います。



インターネットコンテンツ (HTTP) のスキャン

この領域では、インターネットコンテンツ（HTTP）のスキャンに関する設定を行う事ができます。

- **インターネットコンテンツ (HTTP) のスキャン**: ウェブサイトを閲覧する際に指定したポート経由のデータトラフィックを監視し、問題のあるデータがPCに読み込まれた段階で、そのウェブページのデータの読み込みをストップし、それ以上のデータ受信を防ぎます。ウェブサイトに有害スクリプトが埋め込まれている場合などに有効です。プロキシ利用環境では、ポートを指定する必要があります。デフォルトでは80に設定されています。
  G Data EndpointProtection に搭載されている **ウェブコンテンツコントロール** 機能を使用する場合は、この機能を有効にする必要があります。

- **ブラウザのタイムアウトを防止**: ウェブコンテンツを表示する際に発生するブラウザのタイムアウトエラー表示を回避します。**インターネットコンテンツ (HTTP) のスキャン**を有効にすると、環境によっては、ウェブコンテンツの表示に遅れが生じる場合があります。その際は、この機能を有効にして、ブラウザのエラー表示を回避できます。
- **ダウンロードの容量制限**: 特定のデータ量を持つウェブコンテンツで、スキャンを中断します。スキャン中断の設定値を指定します。これは、大容量ファイルのダウンロード時に実行されるスキャンによって発生する可能性のある遅延を回避するために有効です。

- **ウェブ保護の例外**: 特定ウェブサイトをホワイトリストに追加し、ウェブ保護によるスキャン処理が実行されないように設定します。

インスタントメッセンジャー

この領域では、インスタントメッセーンジャーのトラフィックのスキャンに関する設定を行う事ができます。

- **IMトラフィックをスキャン**: インスタントメッセンジャー経由で送信されるウイルスや不正ファイルのダウンロードをブロックします。インスタントメッセンジャーが標準的なポートを使用していない場合は、サーバーのポート番号に適切なポートアドレスを入力します。

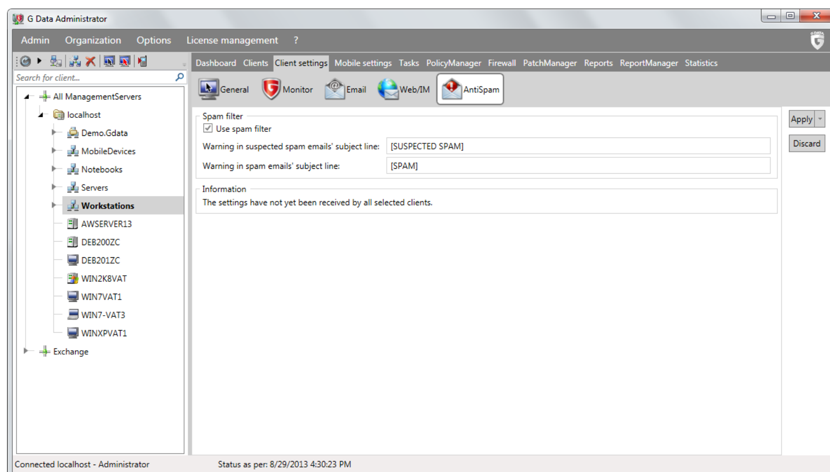
- **IMアプリケーションへの統合 - IMアプリケーションがある場合**: Microsoft Messenger（バージョン 4.7以降）もしくはTrillian （バージョン 3.0以降）を使用している場合、ここにチェックを入れると、コンテキストメニューからウイルススキャンを実行できるようになります。

バンクガード

バンクガードはオンラインバンキングの際に効果を発揮する機能です。ネットワークライブラリの有効性をチェックし、未知のバンキング系トロイの木馬による改ざんを未然に防ぎます。この機能は、Internet Explorer , Firefox , Chrome を使用しているコンピュータで利用可能です。

アンチスパム

スパムフィルタを使用にチェックを入れると、クライアントが送受信するメールから、スパムメールを検出します。スパムメールもしくはスパムの疑いがあるメールには、件名に警告文字を指定し挿入できます。



メーラー上で振り分け用のルールを定義することで、件名に [スパム] とある メールを、自動的にゴミ箱もしくはスパムメール専用フォルダに移動することも可能です。

※アンチスパム機能は、G Data ClientSecurity Business / G Data EndpointProtection Business にのみ搭載されています。

モバイル設定

モバイル設定のタブからは、モバイルデバイス用の管理機能へ簡単にアクセスできます。G Data Internet Security for Android アプリを Android 端末にインストールして端末側で ManagementServer との接続設定を行うと、G Data Administrator のクライアント管理領域に当該端末が表示されるようになります。

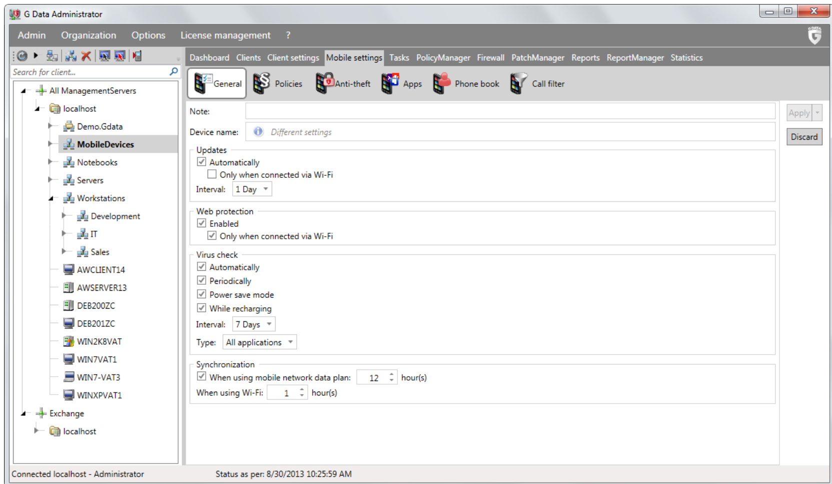
モバイル設定内の機能は、モバイルのクライアント（もしくはグループ）を選択した際に利用できます。

モバイル設定内で設定した各項目は、端末と ManagementServer が同期された後に反映されます。設定変更後にクライアントへの同期が行われていない間は、クライアントは古い設定のまま動作しますのでご注意ください。

一般

一般タブでは自動更新やウェブ保護、ウイルススキャン、同期の設定を行う事ができます。また、この画面では、端末識別用に以下の情報を登録する事ができます。

- **コメント**: モバイル端末に関する情報
- **端末名**: モバイル端末の名前



更新

この領域では更新に関する設定を行う事ができます。

- **自動**: モバイル端末用アプリの更新を自動更新で行うかどうか選択することができます。自動を選択した場合は、更新間隔の設定や、更新の実行をWi-Fi接続時のみに制限することができます。

ウェブ保護

この領域では、ウェブ保護に関する設定を行う事ができます。

- **ウェブ保護**: ウェブ保護を有効にすると、インターネットへのアクセスする際にモバイル端末を保護することができます。ウェブ保護では、ウェブトラフィックの監視を常に行うか、あるいはWi-Fi接続時に限定して行うかを設定できます。

ウイルススキャン

この領域ではアプリインストール時のウイルススキャンや、定期的なウイルススキャンに関する設定を行う事ができます。

- **自動スキャン**: 新しくアプリがインストールされた際にスキャンを自動実行します。

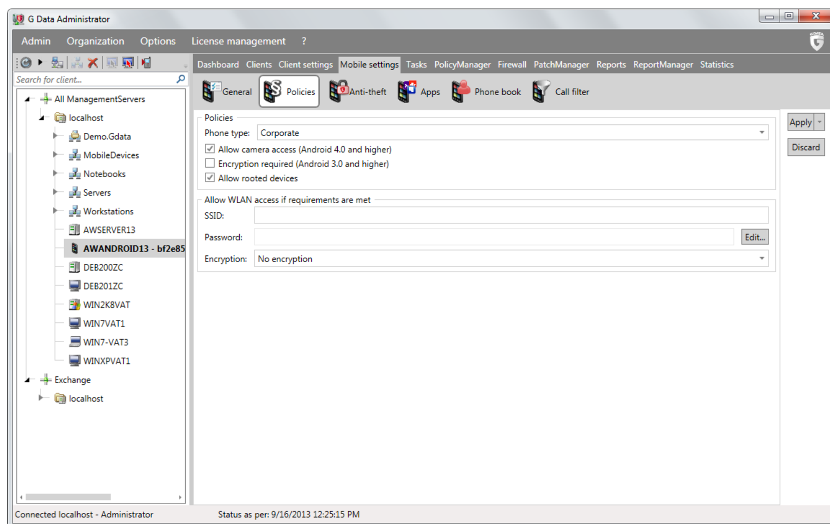
- **定期スキャン**: スキャンを自動で実行します。**頻度**の項目でスキャン間隔も設定可能です。
- **省エネモード**: 端末のバッテリー残量が僅かな場合、バックグラウンドスキャンを実行しません。
- **充電時にスキャン**: 端末が充電中の場合にバックグラウンドスキャンを実行します。
- **種類**: スキャン対象を**すべてのアプリ**もしくは**インストール済みアプリ**から選択できます。

同期

この領域では、マネジメントサーバーとモバイルクライアントを同期する間隔を設定できます。同期のための接続間隔は、Wi-Fi接続時、データ通信接続時それぞれに設定する事ができ、チェックを外すことで、データ通信接続時は同期を行わないように設定する事も可能です。

ポリシー

ポリシータブではモバイル端末の種類を設定し、その種類によって運用ポリシーを設定できます。必要に応じて端末の機能を制限する事ができ、会社用の端末と、社内ネットワークを保護することができます。



ポリシー

ポリシータブでは、**端末の種類**から、選択した端末に割り当てるポリシーの種類を選択します。会社支給の端末には、**コーポレート**を選択することをお勧めします。**コーポレート**に設定すると、端末の様々な機能がユーザー自身で変更できないように制限を掛けて管理することができるようになります。端末の種類に依存することなく、以下の機能を制御することができます。

- **カメラへのアクセスを許可**(Android 4.0 以降): 端末のカメラへのアクセスを許可します。
- **暗号化が必要**(Android 3.0 以降): 自動で Android の暗号化設定ウィンドウを開き、 端末ユーザーに端末の暗号化を促します。端末側で暗号化が有効でない、データ削除などの機能が利用できません。
- **ルート化された端末を許可**: ルート化された端末の利用を許可/拒否します。このオプションを無効化すると、**盗難対策** で設定したパスワードを用いて、ルート化された端末が使用できないようにブロックされ、**Wi-Fiへのアクセスを許可**で定義したWi-Fiにアクセスすることもできなくなります。

Wi-Fiへのアクセスを許可

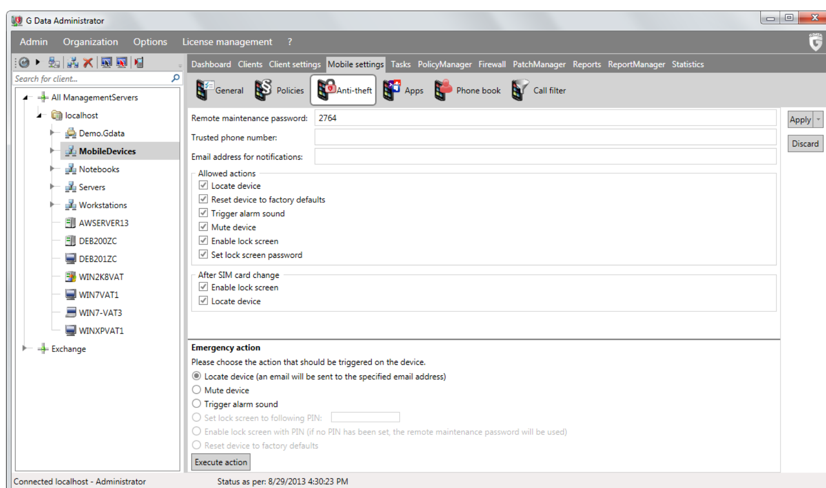
ルート化された端末のため、特定Wi-Fiへのアクセスをブロックでき、セキュアに管理された端末のみ社内Wi-Fiへのアクセス許可できるように設定できます。

アクセス許可する社内用Wi-Fiの SSID を指定してください。Wi-Fi が暗号化されている場合は、**暗号化** を選択して**パスワード**を入力してください。

盗難対策

盗難対策タブでは、紛失盗難時に端末や端末内のデータ保護に役立つ様々な機能が含まれています。紛失/盗難時は、特定の電話番号から**SMSコマンド**を送信することで、リモートロック、データ消去、位置特定ができます。また、Google Cloud Messaging を使うと、これらの機能がマニュアル操作でいつでも起動できます。

盗難対策を設定するには、一般設定を行う必要があります。まず、PINコードとして機能する **リモート操作用パスワード** (連続しない数字のみで構成) を設定してください。このパスワードは、SMSコマンド送信時に一緒に含めて入力する必要があるので、第三者が不正にリモート操作を行わないよう厳重に管理してください。**リモート操作用パスワード** をリセットするには、**信頼できる電話番号**に設定した電話番号から送信する必要があります。特定コマンドではレポートやその他の通知メッセージが生成されます。この通知メッセージの受け取るためのメールアドレスは、**通知先メールアドレス**欄に入力してください。



許可された操作

許可された操作領域では、SMSで起動する盗難対策の操作を定義することができます。これらの操作は、対象端末に対して**リモート操作用パスワード**を含むSMSコマンドを送信して行います。

SMSコマンド一覧:

以下は、端末にSMSで送信できるコマンド一覧です。コマンドへの回答は通常、SMSコマンドの送信元デバイスに送信されます。メールアドレスでの返答が行われるコマンドは、**通知先メールアドレス**に登録したメールアドレスに結果が送信されます。

※ コマンド（太字）とパスワード（斜体）の間には半角スペースを入力する必要があります。
※ コマンド内の半角スペースや記号も間違いなく入力する必要があります。

入力例
1234をパスワードとし、位置情報送信のコマンドを送る場合
1234 locate　(文字で記載すると　1234半角スペースlocate　となります)

- **端末の位置を確認**: 端末が自身の位置情報を指定メールアドレス宛てにメール送信します。このコマンドを実行するには、対象端末に次の内容でSMSを送信します。
  SMSコマンド:　*SMSコマンド用パスワード* **locate**
- **端末を工場出荷時の状態にリセット**: 端末を工場出荷時の状態にリセットします。端末内の全データは消去されます。このコマンドを実行するには、対象端末に次の内容でSMSを送信します。
  SMSコマンド:　*SMSコマンド用パスワード* **wipe**
- **警告音を鳴らす**: Internet Security を起動するまで、端末が警告音を発し、端末を紛失した場所を見つけるのに役立ちます。このコマンドを実行するには、対象端末に次の内容でSMSを送信します。
  SMSコマンド:　*SMSコマンド用パスワード* **ring**
- **端末をミュートに設定**: 端末を無音に設定します。位置を確認する際の着信音はここでは除外されます。このコマンドを実行するには、対象端末に次の内容でSMSを送信します。
  SMSコマンド:　*SMSコマンド用パスワード* **mute**
- **画面ロックを有効にする**: 端末スクリーンをロックする事で不正利用を防ぎます。このコマンドを実行するには、対象端末に次の内容でSMSを送信します。
  SMSコマンド:　*SMSコマンド用パスワード* **lock**
- **画面ロック用のパスワードを設定**: 画面ロックされた状態から端末をアンロックするためのパスワードを忘れた場合など、パスワードを再設定できます。このコマンドを実行するには、対

象端末に次の内容でSMSを送信します。
SMSコマンド: *SMSコマンド用パスワード* set device password: *画面ロックに使用するパスワード*

- **パスワードのリセット**: **リモート操作用パスワード**をリモートで変更するには、**信頼できる電話番号** に設定した端末宛てに次の内容でSMSを送信してください。
  SMSコマンド: remote password reset: *新しいSMSコマンド用パスワード*

SIMカード交換後

G Data のアプリのインストール時点のSIMカード情報が記憶されます。インストール後、端末に挿入されているSIMが不正に交換された場合（例: 盗難時など）、特定の操作を自動起動させることができます。

- **画面ロックを有効にする**: **許可された操作**のオプションと同一の機能です。
- **端末の位置を確認**: **許可された操作**のオプションと同一の機能です。

緊急時の機能

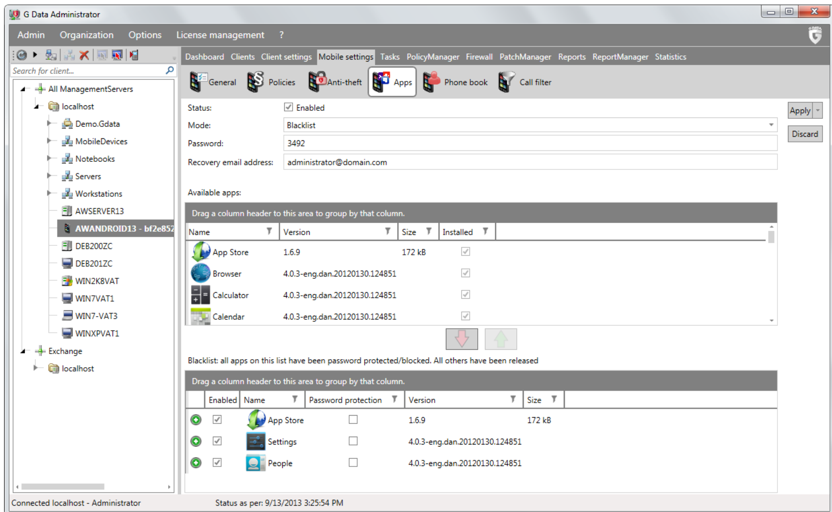
インターネットベースの Google Cloud Messaging を使って、緊急操作を起動できます。これはSIMカードなしの端末でも機能します。Google Cloud Messaging は、まず事前に設定を行う必要があります。設定後は、**オプション** > **サーバー設定** > **Mobile** で**送信者 ID** と **API キー**を入力してください。次に操作を選択して、**操作を実行**をクリックすると、ターゲットの端末に即コマンドが送付されます。

- **端末の位置を特定**: **許可された操作**と同一の機能です。
- **端末をミュートに設定**: **許可された操作**と同一の機能です。
- **警告音を鳴らす**: **許可された操作**と同一の機能です。
- **画面ロック用の PIN を設定**: **許可された操作**と同一の機能です。
- **PIN を使って画面ロックを有効にする**: **許可された操作**と同一の機能です。
- **端末を工場出荷時の状態にリセット**: **許可された操作**と同一の機能です。

アプリ

アプリタブでは、選択した端末でのアプリへのアクセスを設定します。アプリをブロック/許可するには、フィルタが**ブラックリスト**もしくは**ホワイトリスト**モードを利用するか選んでください。ブラックリストモードでは、ブラックリストに登録した全アプリがブロックされる、もしくはパスワード保護されます。ブラックリスト以外のアプリはすべてアクセスできます。

一方、ホワイトリストモードでは、登録された全アプリが許可される、もしくはパスワード保護されます。ホワイトリスト以外のアプリはすべてブロックされます。**パスワード**（PINコード）は、ブロックされたアプリにアクセスするためのものです。**メールのリカバリ**では、パスワード紛失時にパスワード送付先のメールアドレスを設定できます。

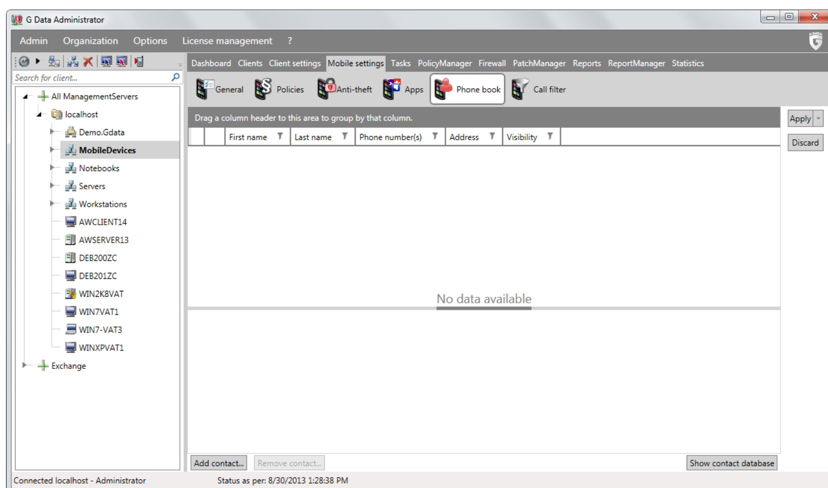


利用可能なアプリでは、クライアント選択領域で選択した端末にインストール済みのアプリがすべて表示されます。それぞれのアプリは、アプリ名、バージョン、アプリ容量、インストール日を確認する事ができます。アプリをホワイトリストもしくはブラックリストに移動させるには、矢印ボタンを使って行います。ホワイトリスト/ブラックリストに移動したアプリは、**パスワード保護**をでロックをかける事ができます。

連絡帳

連絡帳タブでは、より高度な連絡帳管理ができます。連絡先はG Data のアプリから連絡帳へ新規追加でき、端末デフォルトの連絡帳上で非表示化などの設定も可能です。更に、**アプリ**でAndroid端末デフォルトの連絡帳をブロックすることで、デフォルト連絡帳の代わりとして中央管理できる連絡帳として運用することもできます。

画面中央の領域では、G Data Internet Security アプリの連絡帳に追加された連絡先がすべて表示されます。各連絡先は、姓、名、電話番号および住所などが表示されます。表示ドロップダウンメニューでは、G Data アプリで追加した連絡先の表示をAndroid 連絡帳上でどのように表示するか（**表示**もしくは**非表示**）設定できます。更に、**非表示の通信**で通話やSMSを非表示化させる事も可能です。

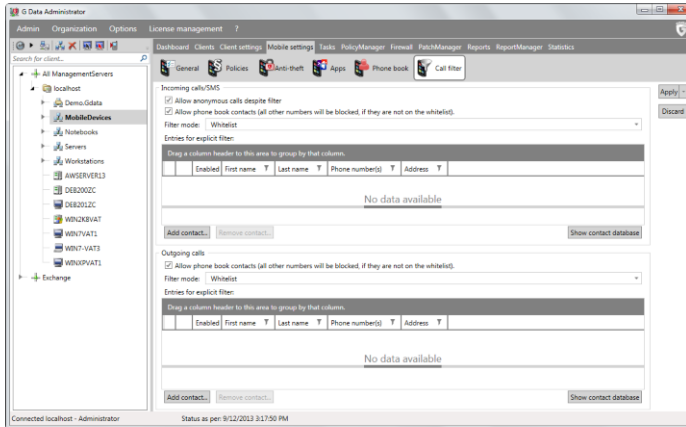


連絡帳に連絡先を追加するには、**連絡先を追加**をクリックします。連絡先データベースウィンドウ内に定義された全連絡先が表示されます。連絡先を選択して、**選択**をクリックして連絡帳に追加します。連絡先を取り除くには、**連絡先を取り除く**をクリックします。

連絡先データベースに連絡先を追加するには、ツールバーの**連絡先を作成**アイコンをクリックするか、**連絡先をインポート**でActive Directory Organizational Unit (OU)から連絡先をインポートします。連絡先の作成時（※）は、姓名のほか、住所、メールアドレス、電話番号、ファックス番号、組織名なども入力できます。※少なくとも「姓」もしくは「名」を必ず入力する必要があります。連絡先データベースから連絡先を取り除くには、対象を選択してツールバー上の**削除**アイコン、もしくは右クリックメニューの**削除**を選択してください。

通話フィルタ

通話フィルタでは、着信（通話とSMS）および発信（通話のみ）をフィルタを設定できます。**連絡帳**タブと同様、連絡先をブラックリストもしくはホワイトリストに追加やフィルタ定義などができます。



着信通話/受信SMS

着信通話/受信SMS 領域では、モバイルクライアントがインストールされた端末に着信する電話やSMSに対してのフィルタリング方法を設定できます。

フィルタを無視して、非通知番号からの着信を許可のチェックを外した場合は非通知の着信をすべてブロックします。**連絡帳の電話番号をすべて許可** のチェックを入れた場合は連絡帳に含まれる電話番号からの着信はすべて許可されます。

フィルタモードには、フィルタ用エントリに追加された電話番号からの着信を許可する**ホワイトリスト**、フィルタ用エントリに追加された電話番号からの着信をブロックする**ブラックリスト**の2つの種類があります。

連絡先を追加をクリックすると、連絡先データベースに存在する連絡先を選択し、フィルタ用エントリに追加する事ができます。そこで追加した連絡先をフィルタ用エントリから取り除くには、**連絡先を取り除く** をクリックします。

発信通話

発信通話領域では、モバイルクライアントがインストールされた端末が発信する電話やSMSに対してのフィルタリング方法を設定できます。

連絡帳の電話番号をすべて許可 のチェックを入れた場合は連絡帳に含まれる電話番号への発信はすべて許可されます。

フィルタモードには、フィルタ用エントリに追加された電話番号への発信を許可する**ホワイトリスト**、フィルタ用エントリに追加された電話番号への発信をブロックする**ブラックリスト**の2つの種類があります。

連絡先を追加をクリックすると、連絡先データベースに存在する連絡先を選択し、フィルタ用エントリに追加する事ができます。そこで追加した連絡先をフィルタ用エントリから取り除くには、**連絡先を取り除く**をクリックします。

この機能で発信をブロックした場合は、端末利用者は管理者にブロック解除を申請する事ができます。その場合、G Data Administrator の **レポート**画面にブロックの履歴が表示されますので、そこから対象の連絡先をホワイトリストもしくはブラックリストに追加してください。

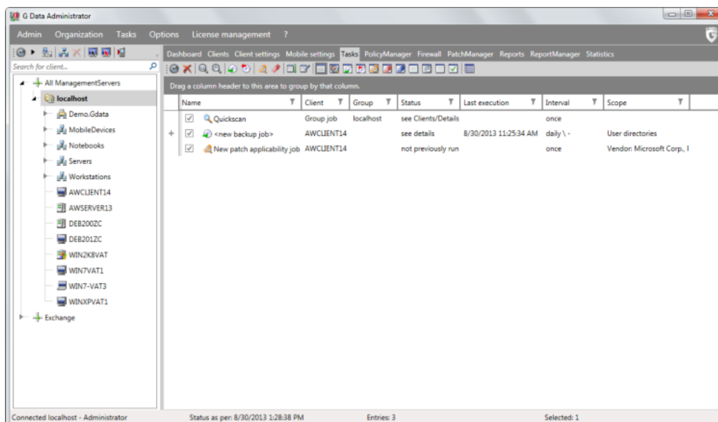
タスク

タスクでは、G Data Security Client をインストールした対象クライアントへのスキャンタスクを設定できます。タスクには、指定した日時に1 回のみ実行する**スキャンジョブ（ワンタイム）**と定期的に実行する**スキャンジョブ（スケジュール）**の2種類があります。それぞれのジョブは複数作成する事ができますので、PC環境や利用状況に合わせてジョブ設定を行ってください。

一覧には、設定済みのスキャンジョブが表示されます。**名前**や**コンピュータ**などの項目をクリックすると、項目別で表示を並び変えることができ、並び替えが適用されている項目には、小さな矢印マークが表示されます。

- **名前**: スキャンジョブに付与された名前が表示されます。

- **クライアント**: クライアントPCの名前が表示されます。
- **グループ**: ジョブが割り当て先グループの名前が表示されます。グループにスキャンジョブを割り当てると、一覧では個々のコンピュータ名は表示されず、グループ名だけが表示されます。
- **ステータス**: スキャンジョブのステータスまたはスキャン結果が表示されます。
- **最終実行**: スキャンジョブが最後に実行された日時が表示されます。
- **間隔**: スケジュール設定したジョブを繰り返す間隔が表示されます。
- **スキャン範囲**: スキャン対象 (例: ローカルハードディスク) が表示されます。



タスクの管理は、タスクリストの上にあるツールバーに表示される以下のアイコンから直接操作できます。

 **更新**: 表示結果を更新します。最新のジョブリストをG Data ManagementServer から取得します。

 **削除**: 選択したジョブを削除します。

 **スキャンジョブ（ワンタイム）**: 一度のみ実行するスキャンジョブを作成できます。アイコンをクリックすると、ウィンドウが表示されるので、タブで分類されている各項目を設定してスキャンジョブを作成します。既存のスキャンジョブの設定を変更するには、対象のスキャンジョブをダブルクリックするか、右クリックして**プロパティ**を選択します。

 **スキャンジョブ（スケジュール）**: 定期的に実行するスキャンジョブを作成します。アイコンをクリックすると、ウィンドウが表示されるので、タブで分類されている各項目を設定してスキャンジョブを作成します。既存のスキャンジョブの設定を変更するには、対象のスキャンジョブをダブルクリックするか、右クリックして**プロパティ**を選択します。

 **今すぐ実行する**: 元々の設定時間に関係なく、選択したジョブをすぐに実行します。例えば、実行済みスキャンやキャンセルされたスキャンをすぐに再実行できます。

 **ログを表示**: タスクに関するログ情報を呼び出します。

 **すべてのタスクを表示**

 **スキャンジョブのみ表示**

 **スキャンジョブ（ワンタイム）のみ表示**

 **スキャンジョブ（スケジュール）のみ表示**

 **未実行のスキャンジョブのみ表示**

 **実行済みのスキャンジョブの未表示**

 **グループジョブを詳細表示**: グループジョブ関連のアイテムをすべて表示します。このオプションはグループ選択時のみ利用できます。

タスクモジュールを選択すると、 メニューバー上に追加メニュー **タスク** が表示されます。タスクメニューでは、次の機能が利用できます。

- **表示**: 表示させるジョブについて設定します。**グループジョブを詳細表示**にチェックを入れると、複数のクライアントを含むグループに適用されているスキャンジョブで、すべてのクライアントに関する詳細情報を表示させることができます。

- **今すぐ実行する**: 元々の設定時間に関係なく、選択したジョブをすぐに実行します。
- **キャンセル**: 実行中のジョブをキャンセルします。
- **削除**: 選択したジョブを削除します。
- **新規**: 新規スキャンジョブを作成します。スキャンジョブは、スキャンジョブ（ワンタイム）もしくはスキャンジョブ（スケジュール）のいずれかを選択できます。

スキャンジョブ

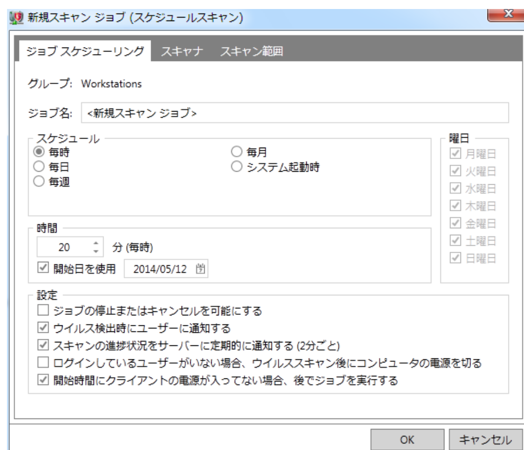
スキャンジョブウィンドウではスキャンジョブに関わる各種設定を行う事ができます。

ジョブスケジューリング、**スキャナ**、**スキャン範囲**タブを選択する事でそれぞれの設定画面へ移動します。

ジョブ スケジューリング

ジョブスケジューリングでは、ジョブ名、スキャンの実行時間（ワンタイムスキャンジョブ）や実行間隔（スケジュールスキャンジョブ）を設定できます。スケジュールスキャンで表示される**システム起動時**のオプションを選択すると、PC起動時にのみスキャンを実行します。クライアントユーザー側にスキャンの一時停止やキャンセルできる権限を付与することもできます。

スキャンの進捗状況をサーバーに定期的に通知する を有効にすると、スキャンのステータスを2分ごとに G Data ManagementServer に報告されます。
ログインしているユーザーがいない場合、ウイルススキャン後にコンピュータの電源を切る を使うと、管理の手間を軽減できます。
開始時間にクライアントの電源が入っていない場合、後でジョブを実行 にチェックを入れると、スケジュールスキャン実行時に対象クライアントが電源がオフの場合、スキャンジョブを後で再実行できます。

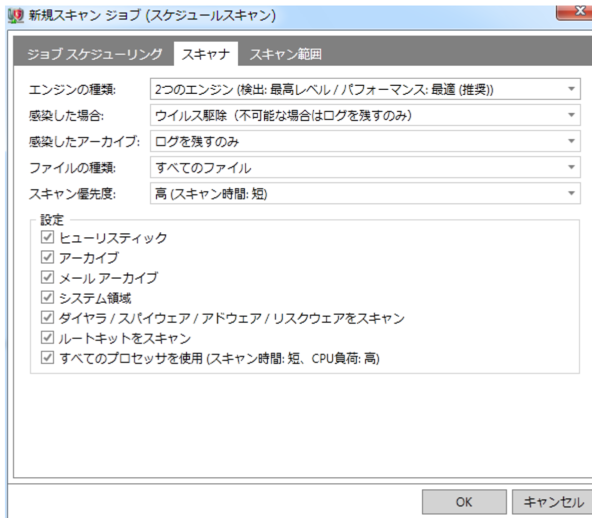


スケジュールスキャンでは、スキャン実行日時や間隔を設定できます。スケジュールスキャンで表示される**システム起動時**を選択すると、スケジュール設定した内容を無視してPC起動時にのみスキャンが実行されるようになります。**毎日**を選択すると、**曜日**での入力値に基づき、指定した曜日や時間でスキャンを実行します。

スキャンジョブ（ワンタイム）では、**次の開始時間を使用**のオプションが表示されます。ここにチェックを入れない場合、作成したスキャンジョブは作成直後に開始されます。指定した曜日を選択すると、更に曜日を選択できるようになります。

スキャナ

スキャナでは、スキャンジョブで適用する設定を定義できます。



ここで設定できるオプションは以下の通りです。

- **エンジンの種類**: G Data は、2種類のウイルス検索エンジンを搭載し、最適なウイルス保護を実現しています。通常は、**2つのエンジン （検出:最高レベル/パフォーマンス:最適（推奨））**を選択してください。1種類のエンジンだけでの稼動も可能ですが、ウイルス保護性能が若干落ちます。1種類のエンジンは、コンピュータのパフォーマンスに問題がある場合にのみ、ご使用ください。

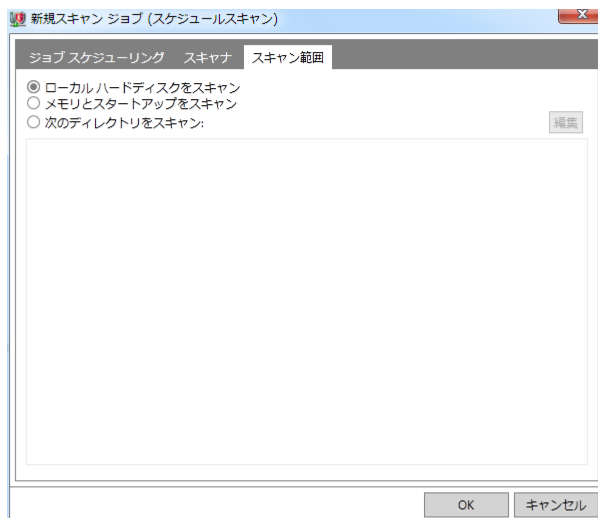
- **感染した場合**: ファイルでウイルス感染が検出された際の処理方法を選択します。処理方法には様々な方法がありますが、コンピュータの使用用途に応じて選択してください。なお、**ファイルを隔離**すると、ファイルは暗号化処理され、ウイルス拡散からシステムを安全に保護できます。一旦、隔離されたファイルは、G Data Administrator から処理操作（ウイルス駆除、削除、元の場所に戻す、**セキュリティラボ** に送付など）を指示できます。
- **感染したアーカイブ**: アーカイブで検出したウイルスを通常のケースとは別の方法で処理します。アーカイブ内のウイルスは通常、アーカイブが解凍されなければ被害が発生しません。
- **ファイルの種類**: スキャン実行対象のファイルの種類を選択します。コンピュータ上の全ファイルをスキャンすると環境によっては非常に時間が掛かります。

- **スキャン優先度**: ウイルススキャンの優先度を、**高、中、低** から選択します。使用環境に応じて、設定してください。（例： スキャン優先度を高に設定すると、スキャン処理が速くなりますが、他のアプリケーションの処理速度は遅くなります）
- **設定**: ウイルススキャンの分析機能を選択します。機能によっては、パフォーマンスに影響を与えるものもあります。使用環境に応じて、適切な設定を選択してください。以下のオプションが利用できます。
  - **ヒューリスティック**: ウイルスが持つ特徴に基づいて未知のウイルスを検出します。
  - **アーカイブ**: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードによる監視が常時オンの場合には、アーカイブを解凍する時にアーカイブ内のウイルスは検出されるので、この機能は無効にしておきます。アーカイブは、クライアントユーザーがPCを集中的に利用していない時間帯などに、定期的に実行することをお勧めします。
  - **メールアーカイブ**: メールアーカイブ内の圧縮ファイルをスキャンします。アーカイブのスキャンを実行すると、スキャンに大変な時間を要します。ウイルスガードがシステム全体で有効になっている場合は、この設定は無効にしてください。
  - **システム領域**: ブートセクターやマスターブートレコードなどのコンピュータのシステム領域をスキャンします。システム領域は、ウイルススキャンの対象に必ず入れることをお薦めします。
  - **ダイヤラ / スパイウェア / アドウェア / リスクウェアをスキャン**: ダイヤラ、スパイウェア、アドウェア、キーロガーなど、ユーザーに様々な損害を与える危険性のある不正プログラムをスキャンします。これらの不正プログラムは、ユーザーの気づかないところで、高額な接続先に接続したり、ユーザーのインターネット閲覧履歴やパスワードやキーストロークを記録し、その情報を第3者に送信します。
  - **ルートキットをスキャン**: ルートキットとは、従来のウイルス検出方法では検出が困難な不正プログラムです。この機能を使うと、ハードディスク内の全データをスキャンすることなく、ターゲットをルートキットに絞ってスキャンします。
  - **すべてのプロセッサを使用**: マルチコアなど複数プロセッサコアを搭載するPCで、スキャンを効率的に処理し、スキャンを高速化します。この機能を有効にすると、コンピュータで稼働中のアプリケーションの処理速度に影響を及ぼす可能性があります。クライアントPCのユーザがコンピュータが利用していない時間帯などに利用することをお勧めします。

スキャン範囲

スキャン範囲では、スキャンの対象を指定できます。範囲を指定すると、仕様頻度の低いアーカイブを含むディレクトリを除外して、特定ディレクトリだけをピンポイントでスキャンしたり、スキャンを分類してジョブを細分化できます。

> **Linux ファイルサーバーのスキャンジョブにおける留意点：**
> ディレクトリの選択では、ルートドライブ ("/") およびすべての共有ディレクトリが表示されます。



ポリシーマネージャー

ポリシーマネージャーは、 会社ポリシーの遵守などに貢献する機能です（G Data EndpointProtection Business のみ搭載）。

この機能を使用すると、デバイスやアプリケーションへのアクセス、インターネットの利用ポリシーを簡単な操作で制御できます。例えば、アクセスを許可するウェブサイトの設定、コンピュータに接続できるデバイスの設定（例：USBメモリ、外付けハードディスク）、コンピュータで使用できるアプリケーションの設定、といった事が可能です。

アプリケーションコントロール

アプリケーションコントロールでは、特定のアプリケーション、ファイル、フォルダの利用を制御できます。

ステータスでは、ポリシーマネージャーの各機能による制限を、クライアントPCを使う全ユーザーアカウントに対して適用するか、管理者権限を持たないアカウントに対してのみ適用するか、または有効にしないかを設定できます。ステータスには、以下の3種類が利用できます。

- **ユーザーに対して有効:**
  Administrator 以外のアカウントで制限が有効になります。

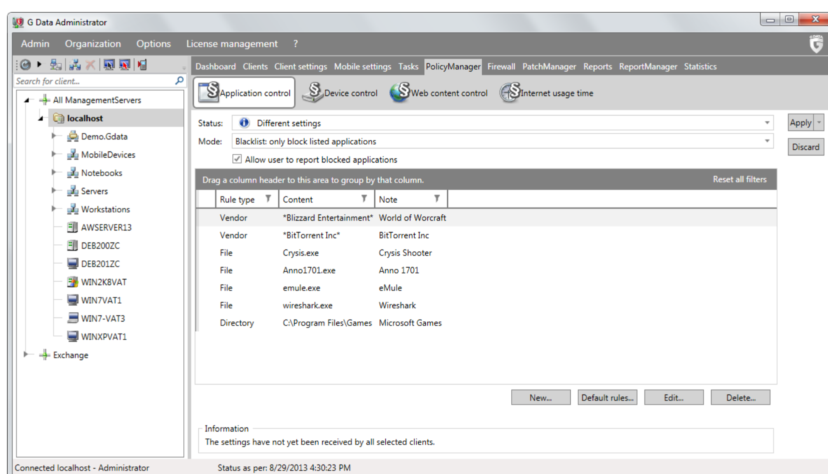
- **ユーザーとアドミニストレーターに対して有効:**
  すべてのアカウントで制限が有効になります。

- **無効:**
  機能が無効になります。

ステータスの下に位置する、**モード**では、アプリケーションコントロールのリストをホワイトリストかブラックリストどちらの方式で運用するか選択できます。

- **ホワイトリスト**: このモードでは、ホワイトリストで許可したアプリケーション/ファイル/フォルダのみ利用できます。

- **ブラックリスト**: このモードでは、ブラックリストでブロックしたアプリケーション/ファイル/フォルダが利用できなくなります。



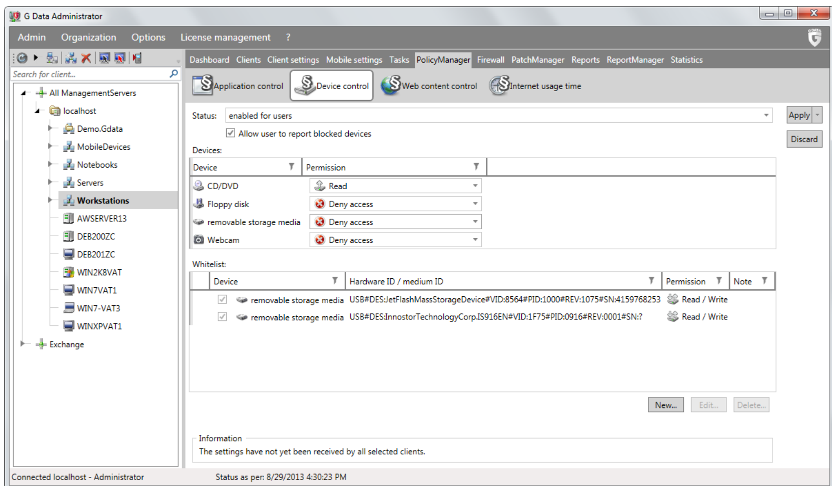
新規ルールを作成するには、[**新規**] をクリックします。ルールは、**開発元**、**ファイル**、**ディレクトリ**の3種類から選択できます。

- **開発元**: アプリケーションの開発元に関する情報を入力し、そのアプリケーションの利用許可/拒否を設定します。開発元の名前を直接入力するか、入力欄の右側に位置する [...] から対象を選択して、開発元の情報を読み込めます。

- **ファイル**: 特定プログラムへのアクセス許可/拒否を設定できます。設定するには、プログラムのファイル名を直接入力するか、[**ファイルのプロパティを取得**] から特定のファイルを探し出すこともできます。ファイル名、製品名、Copyrightの欄では、文字列の前後にアスタリスク「*」を挿入すると、特定文字列に代わるワイルドカードとして使用できます。
- **ディレクトリ**: 特定のディレクトリ（サブディレクトリを含めることも可能）へのアクセス許可/拒否を設定できます。

デバイスコントロール

デバイスコントロールを使用すると、クライアントが接続して利用できるデバイス（例：USBメモリ、CD/DVDドライブ、ウェブカメラなど）の使用を制限できます。



ステータスでは、ポリシーマネージャーの各機能による制限を、クライアントPCを使う全ユーザーアカウントに対して適用するか、管理者権限を持たないアカウントに対してのみ適用するか、または有効にしないかを設定できます。ステータスには、以下の3種類が利用できます。

- **ユーザーに対して有効:**
  Administrator 以外のアカウントで制限が有効になります。

- **ユーザーとアドミニストレーターに対して有効:**
  すべてのアカウントで制限が有効になります。

- **無効:**
  機能が無効になります。

デバイスには、制御可能なデバイスが表示されます。例えば、グループを選択して、グループ内のすべてのクライアント（フロッピードライブの搭載/未搭載にかかわらず）でフロッピードライブの利用を拒否できます。デバイスコントロールでは、以下の権限を定義できます。

 **読み取り / 書き込み**: デバイスに対して、読み込みと書き込みのアクセスができます。

 **読み取り**: デバイスに対して、読み取りのアクセスだけできます。データの書き込みはできません。

 **アクセスを拒否**: デバイスに対して、読み取りと書き込みのアクセスができません。接続されたデバイスは利用できない状態になります。

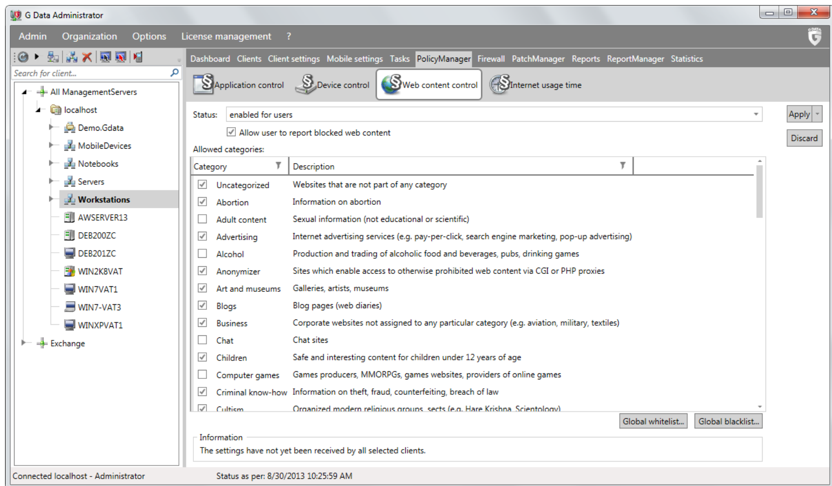
ホワイトリストでは、ブロック済みのデバイスを再び利用できるように制限を解除できます。**[新規]** をクリックすると、利用が制限されているデバイスの一覧が開きます。**[...]** をクリックすると、デバイスを指定して例外を許可することができます。

- **メディアIDを使用**: 特定のCDやDVD（例：会社のプレゼンテーションCDなど）だけをCD/DVDドライブで利用できるように設定します。
- **ハードウェアIDを使用**: ハードウェアに付与されているハードウェアIDの情報をもとに、特定のハードウェア（外付けハードディスク、USBメモリ）だけをネットワーク内で利用できるように設定します。

メディアID、もしくはハードウェアIDを調べるには、**ハードウェアID/メディアID を取得** のダイアログ画面の クライアントからメディア/ハードウェアの使用を許可するクライアントを選択してください。メディア/ハードウェアのID情報は自動的に読み込まれます。**ローカルを検索** からソースの選択を行う事で、ネットワークを管理するPCからメディア/ハードウェアのIDを調べることもできます。

ウェブコンテンツコントロール

ウェブコンテンツコントロールは、特定カテゴリに属するサイトの閲覧を制御する機能です。サイトの閲覧を許可するには、クライアント/グループを選択し、閲覧を許可するカテゴリにチェックを入れます。逆に閲覧を禁止するには、該当するカテゴリでチェックを外してください。ウェブコンテンツコントロールで制御できるコンテンツはカテゴリ分類され、カテゴリ内の情報は世界中のサイトに対応し、常に更新されています。



ステータスでは、ポリシーマネージャーの各機能による制限を、クライアントPCを使う全ユーザーアカウントに対して適用するか、管理者権限を持たないアカウントに対してのみ適用するか、または有効にしないかを設定できます。ステータスには、以下の3種類が利用できます。

- **ユーザーに対して有効:**
  Administrator 以外のアカウントで制限が有効になります。

- **ユーザーとアドミニストレーターに対して有効:**
  すべてのアカウントで制限が有効になります。

- **無効:**
  機能が無効になります。

ホワイトリストは、**許可されたカテゴリ**で定義した設定とは無関係に、全ネットワークを対象に特定のサイトの閲覧を許可します。ホワイトリストにサイトを追加するには、URLでウェブアドレスを入力して、**[追加]** をクリックします。これで入力したサイトがホワイトリストとして登録されます。ホワイトリストにサイトを編集するには、対象を選択して**[編集]** をクリックします。削除するには **[削除]** ボタンを利用してください。

ブラックリストは、**許可されたカテゴリ**で定義した設定とは無関係に、全ネットワークを対象に特定のサイトの閲覧をブロックします。ブラックリストにサイトを追加するには、URLでウェブアドレスを入力して、**[追加]** をクリックします。これで入力したサイトがブラックリストとして登録されます。ブラックリストにサイトを編集するには、対象を選択して**[編集]** をクリックします。削除するには **[削除]** ボタンを利用してください。

インターネット接続時間

インターネット接続時間では、ネットワーク内のコンピュータのインターネットアクセスをグループ（またはクライアント）毎に細かく制御できます。

ステータスでは、ポリシーマネージャーの各機能による制限を、クライアントPCを使う全ユーザーアカウントに対して適用するか、管理者権限を持たないアカウントに対してのみ適用するか、または有効にしないかを設定できます。ステータスには、以下の3種類が利用できます。

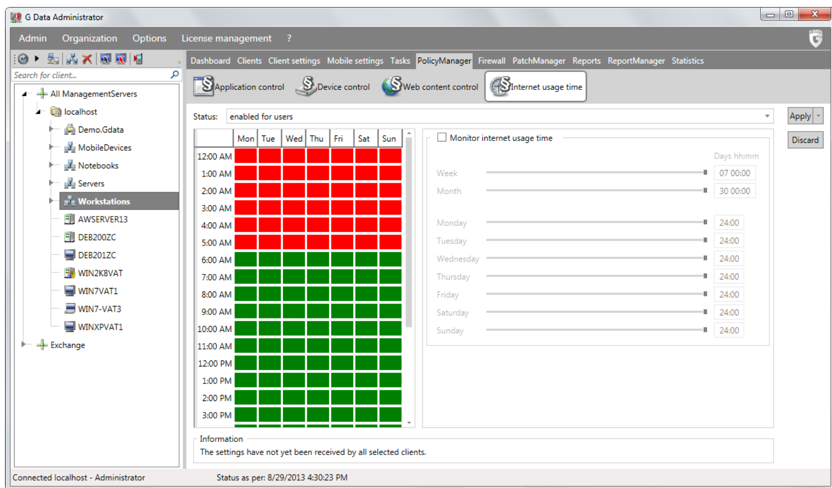
- **ユーザーに対して有効:**
  Administrator 以外のアカウントで制限が有効になります。
- **ユーザーとアドミニストレーターに対して有効:**
  すべてのアカウントで制限が有効になります。
- **無効:**
  機能が無効になります。

インターネット接続時間の設定を行うには、左下の表で対象の時間帯をマークし、表示されるメニュー（**許可する時間**もしくは**禁止する時間**）から選択します。遮断する時間帯は赤色で表示され、許可された時間帯は緑色で表示されます。ユーザーが遮断時間中にインターネットにアクセスすると、ユーザーのブラウザ上でメッセージを表示させ、アクセス拒否を知らせます。

インターネット利用時間を監視にチェックを入れると、月/週/日単位（曜日の指定も可能）でインターネットが利用できる日数と時間数を設定できます。設定はスライダーを左右に移動する事で可能ですが、数値を直接入力する事も可能です。その場合はスライダーの右にある数値欄に [**日 時:分**] の順番で入力します。

例:4日と20時間5分を許可するならば、04 20:05 と入力します。

インターネット利用時間の設定では、常に最小値が適用されます。例えば、1 か月の時間制限を 4 日間と設定する一方で 1 週間の時間制限を 5 日間と設定した場合、このユーザーのインターネット利用時間は、自動的に 4 日間に制限されます。



ファイアウォール

G Data 法人製品に搭載されているファイアウォールは、中央管理可能なファイアウォールです。ファイアウォールのタブを選択すると、ファイアウォール設定の**一覧**や**ルールセット**の設定などが表示されます。

※ファイアウォールは、G Data ClientSecurity Business / G Data EndpointProtection Business にのみ搭載されています。

一覧

G Data のファイアウォールでは、ファイアウォールの稼動モードを次の２種類の設定から選択できます。モードの選択は、**オートパイロット/ルールセット**で行います。

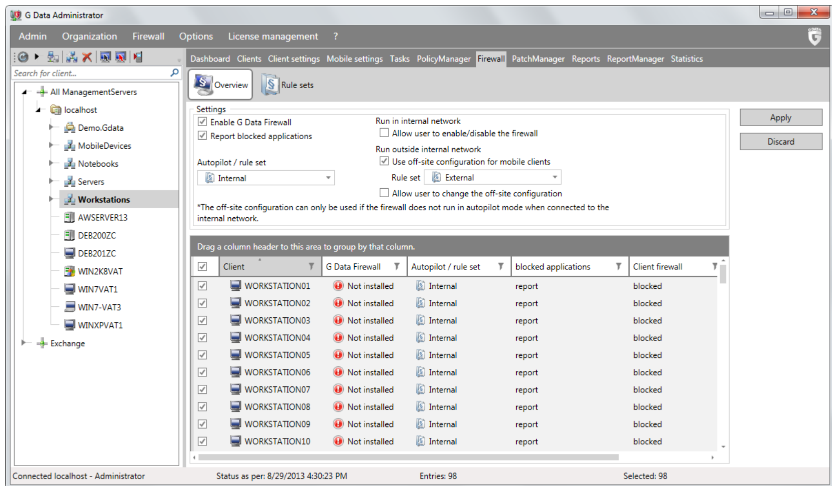
- **オートパイロット**: G Data が設定したデフォルトルールに従って、ファイアウォールをバックグラウンドで自動処理します。ユーザーへの確認は入りません。
- **ルールセット**: ネットワーク環境に応じて、ファイアウォール設定をマニュアルで定義できます。

この画面では、ファイアウォールに関する以下の基本的な設定を行う事ができます。

- **G Data Firewall を有効にする**: 対象クライアント上でファイアウォールを有効にします。このチェックボックスにチェックが入っていない場合は、ファイアウォールは対象クライアント上で無効となります。

- **ブロックしたアプリケーションを通知**: クライアントが G Data マネージメントサーバー と接続されている場合、ファイアウォールによってブロックされたアプリケーションは **レポート** 領域で確認できます。
- **ユーザーによるファイアウォールの有効/無効操作を許可**: クライアントユーザーに対して、ファイアウォールを無効にできる権限を付与します。この設定はクライアントが社内ネットワーク内に存在する場合のみ利用できます。（上級者が使用している環境に対してのみ有効化する事を推奨します）
- **モバイルクライアント用オフサイトコンフィグレーションを使用**: オフサイト（＝特定の場所から離れたの意）コンフィグレーションは、クライアントPCをオフサイト使用（例: 社外ネットワーク）した際のファイアウォール設定です。この設定を利用すると、社外に持ち出されてマネージメントサーバーと接続されていないモバイルPCに対して、適切なファイアウォール設定を適用することができます。オフサイトコンフィグレーションを設定したモバイルPCは、再び社内ネットワークに接続されると、通常の社内ネットワーク用のファイアウォール設定が自動的に適用されます。
- **ユーザーによるオフサイトコンフィグレーションの変更を許可**: ユーザーがオフサイトコンフィグレーション設定を自身で変更できます（上級者ユーザーのみ推奨）。オフサイトコンフィグレーションを設定したモバイルPCは、再び社内ネットワークに接続されると、通常の社内ネットワーク用のファイアウォール設定が自動的に適用されます。

オフサイトコンフィグレーションは、コンピュータが社外ネットワークに接続され、かつファイアウォールがオートパイロットモードに設定されていない場合にのみ、利用できます。社内ネットワーク内のクライアントPCでオートパイロットが設定されている場合は、クライアントがネットワークに接続されていない時もオートパイロットモードが稼動します。



一覧には、すべての（もしくは選択したグループの）クライアントが表示され、各クライアントのファイアウォール設定が確認できます。設定を変更する場合は、対象をクリックして行います。

- **クライアント**: クライアントのコンピュータ名が表示され、対象クライアントに G Data Security Client がインストール済みか確認できます。
- **ファイアウォール**: ファイアウォールのステータス（有効/無効/未インストール）が確認できます。
- **オートパイロット/ルールセット**: 適用されているモード（オートパイロット/ルールセット）が表示されます。
- **ブロックされたアプリケーション: ブロックしたアプリケーションを通知**のオプションの設定（通知する/通知しない）が表示されます。
- **クライアント ファイアウォール: ユーザーによるファイアウォールの操作（有効/無効）が可能**のオプションが設定が表示されます。
- **オフサイトコンフィグレーション**: オフサイト（＝『特定の場所から離れた』の意）コンフィグレーションを選択すると、G Data マネジメントサーバーに接続されていない間は、クライアントユーザーがファイアウォールの設定を自由に管理/設定できます。※オフサイトコンフィグレーションは、コンピュータが社外ネットワークに接続され、ファイアウォールがオートパイロットモードで稼動していない場合にのみ、利用できます。

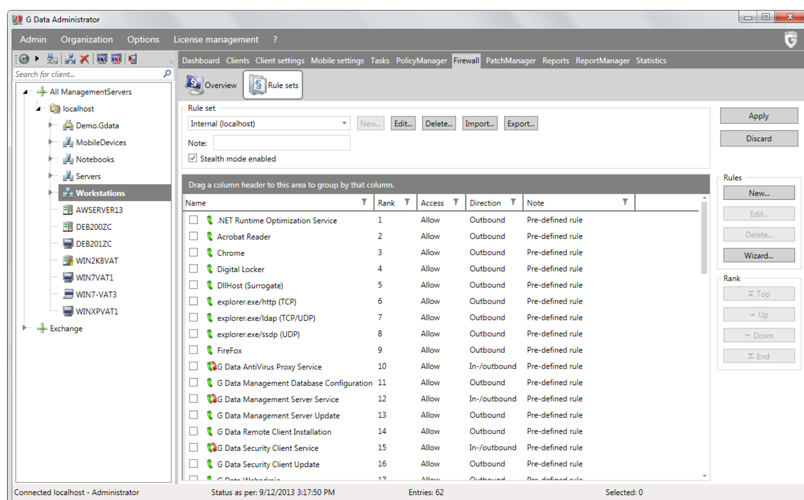
クライアントPCのファイアウォール設定を変更するには、対象をカーソルを合わせて右クリックするか、メニューバー上のファイアウォールを選択します。表示されるメニューで次のオプションを設定できます。

- **ルールセットを生成**: **ルールセット**領域に移動し、新規ルールセットを作成します。

- **ルールセットを編集**: **ルールセット**領域に移動し、クライアントファイアウォールの既存ルールを編集します。
- **G Data Firewall をインストール**: 対象クライアントにファイアウォールをインストールします。
- **G Data Firewall をアンインストール**: 対象クライアントからインストール済みのファイアウォールをアンインストールします。

ルールセット

ルールセットのアイコンを選択すると、それぞれのネットワーク環境に適した設定の作成や適用が行えます。

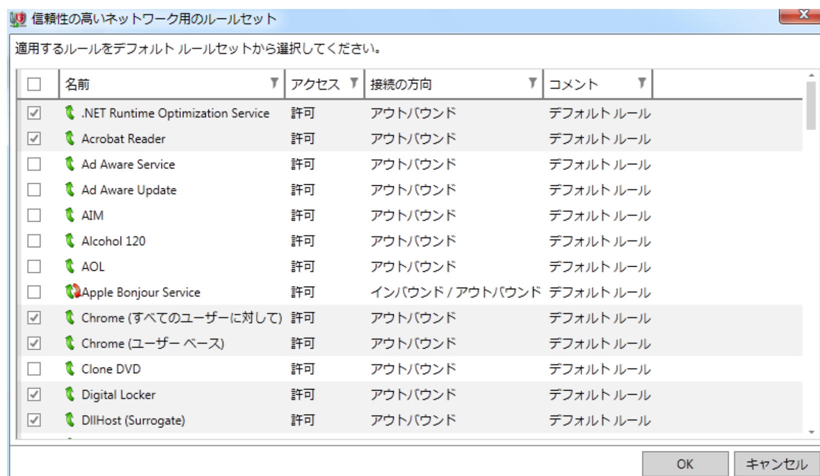


<u>新規ルールセット</u>

ルールセットアイコンの真下にあるルールセット領域では、ファイアウォールルールの**名前**や**ステルスモード**の状況が一覧できます。新規ルールセットを生成するには、［**新規**］ボタンを押します。デフォルトルールを元に新たなルールセットを作成したり、ルールセットをお好みでカスタマイズすることが可能になります。ここで作成したルールセットはXML形式でインポート、エクスポートする事も可能です。

- **新規**: 新しいルールセットを生成できます。

- **ステルスモードを使用**: このモードを使用すると、不正なリクエストでコンピュータのポートに関する情報をブロックでき、攻撃者側にシステム情報を取得されるのを困難にします。



ルールセットは、オフサイトコンフィグレーションのオプションを使用する事で、社内ネットワーク、外部ネットワークそれぞれ異なるルールを設定する事も可能です。例えば、社内では信頼性の高いネットワーク用のルールセットを用意し、ネットワークアクセスの自由度と作業効率を優先。社外では信頼性の低いネットワーク用のルールセットを設定し、セキュリティの厳密さを優先。このように状況に応じて柔軟な設定を行う事ができます。

新規ルールの生成/ルールの編集

作成されたルールはルールセット画面に一覧されます。右のメニューにある［**新規**］、［**編集**］ボタンで、選択中のルールセットへのルールの追加もしくは既存のルールの編集を行う事ができます。

- **名前**: 作成するルール、もしくは作成済みルールの名前です。
- **有効なルール**: ルールの適用・未適用を設定します。ここでチェックを外してもルール自体は削除されません。
- **コメント**: ルールの生成方法が表示されます。デフォルトルール経由で作成されたルールは**デフォルトルール**、ファイアウォールのアラート経由で作成されたルールは**アラートにより作成**、ユーザー自身で新規作成したルールはコメント欄に入力した情報がそれぞれ表示されます。
- **接続の方向**: 許可する接続の方向をアウトバウンド、インバウンド、もしくはアウトバウンド/インバウンドから選びます。
- **アクセス**: ルールセットにおいて、プログラムに適用するアクセスを許可もしくは拒否から選択します。

- **プロトコル**: 接続プロトコルを選択します。特定アプリケーションに関連付けて設定する場合は、［**アプリケーション割当て**］から行います。また同じ要領で、特定ポートを［**インターネットサービス割当て**］で定義できます。
- **時間**: ネットワークリソースへのアクセスを時間ベースで設定します。例えば、会社の稼働時間のみアクセスできるように設定して、それ以外の時間はアクセスを拒否するように設定することができます。
- **IP アドレス範囲**: 固定IPアドレスが付与されているネットワークでは、ネットワークの使用をIPアドレス範囲で制限することをお勧めします。これにより不正な攻撃リスクを削減できます。

ルールウィザード

ルールウィザードを使用すると、ルールセットに新たなルールを追加する事ができます。

ルールウィザードでは以下の操作が可能です。

- **アプリケーションへのアクセスを許可/拒否**: アプリケーションを選択して、ネットワークへのアクセス（許可もしくは拒否）を定義します。定義するには、まずアプリケーション（アプリケーションのパス）を選択します。その後、**接続の方向**をインバウンド、アウトバウンド、またはインバウンド/アウトバウンドのいずれから選びます。これにより、例えば音楽アプリケーションがユーザーの嗜好に関する情報を取得するのを防いだり、プログラムの更新データを配布することをブロックできます。

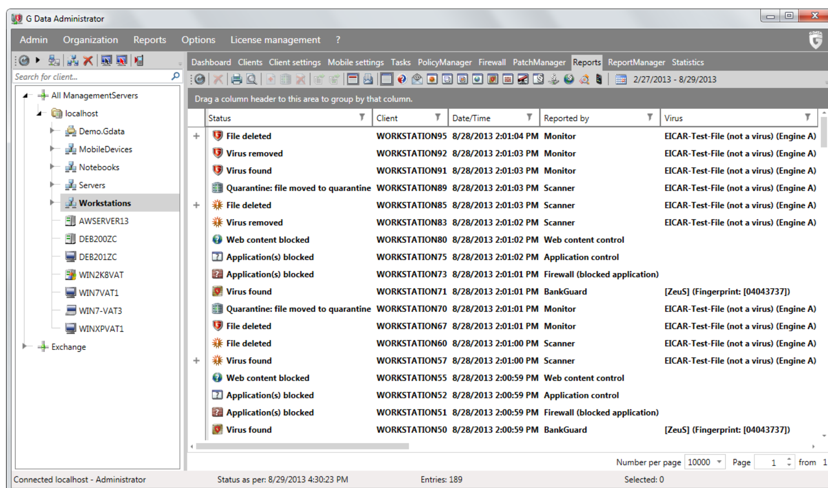
- **インターネットサービス（ポート）を開放/遮断**: ポートを完全にブロックしたり、特定アプリケーションのみに開放したりすることもできます。
- **1つもしくは複数のデフォルトルールを追加**: デフォルトルールとして使用するルールをお好みの設定に変更できます。ここで設定したルールが新規ルール作成時に表示されるようになります。
- **既存のルールをコピー**: 既存ルールのコピーを生成できます。

レポート

ウイルス検出、ポリシーマネージャー（G Data EndpointProtection Businessのみ）、ファイアウォール（G Data ClientSecurity Business / G Data EndpointProtection Business のみ）、システムに関するメッセージ（インストールや再起動など）に関するメッセージが表示されます。

例えばウイルスが検出されると、表示されたアイテムを選択して右クリックするか、ツールバー経由で操作を行うことができます。感染ファイルは削除したり、**隔離フォルダ**へ移動してりすることができます。レポートで表示されるレポートは、条件別に並び替えができます。フィルタが適用されると、適用中の条件は矢印マークが表示されます。並べ替えには、以下の条件が利用できます。

- **ステータス**: 各レポートの重要度や種類をアイコンで表示し、概要の説明をします。
- **クライアント**: レポート対象のコンピュータ名が表示されます。
- **日付/時間**: ウイルスガードによるウイルス検出、もしくはスキャンジョブに関するレポート生成日時が表示されます。
- **検出元**: ウイルスを検出した機能（ウイルススキャン（スキャンジョブ）、ウイルスガード、メールプラグイン）を表示します。
- **ウイルス**: 検出したウイルスが既知の場合、ウイルス名が表示されます。
- **ファイル/メール/コンテンツ**: ウイルスが検出されたファイルもしくは感染の疑いのあるファイルを表示します。メールで検出された場合は、送信者のメールアドレスを表示します。
- **ユーザー**: ウイルス検出時にログオンしていたユーザー
- **詳細**: ファイルのディレクトリ情報を表示します。ディレクトリ情報は、ファイルを隔離領域へ移動した後、元の場所に戻す場合などに重要です。



レポートタブが選択されると、メニューバー上に**レポート**という追加メニューが表示されます。メニューの**レポート**から操作を実行するには、レポート一覧で対象のデータを選択します。選択できる機能は、以下のとおりです。

- **表示**: 表示するレポートの種類を設定します。また、隔離領域の中身を表示させることもできます。
- **関連レポートを非表示**: 複数の異なるジョブやタスクを実行することで発生する、内容が重複するレポートやメッセージを非表示にして、最新のレポートだけが表示されるようになります。
- **既読レポートを非表示**: 既読レポートに関するメッセージ表示の設定を切り換えます。

スキャンジョブにおけるウイルス検出時の対応を、**ログを残すのみ**に設定した場合、検出ウイルスの処理方法を手動で操作できます。操作を行うには、ログに残されたファイルを選択（複数選択も可）し、任意の操作を実行してください。

- **ファイルからウイルスを駆除**: 感染ファイルからウイルスを駆除します。
- **感染ファイルを隔離**: 感染ファイルを隔離領域に移動します。 隔離ファイルは暗号化して G Data ManagementServer の隔離フォルダへ保存され、オリジナルファイルは削除されます。暗号化により隔離ファイルに含まれる感染ファイルは活動ができなくなります。隔離ファイルごとにレポートが作成され、このレポートが削除されると隔離ファイルも一緒に削除されます。感染ファイルのチェックのため、ファイルを G Data セキュリティラボ に送信することもできます。隔離レポート上で右クリックし、表示されるメニューから選択してください。表示されるレポートダイアログでは、送信理由を入力してから［OK］を押してください。
- **ファイルを削除**: クライアント上の感染ファイルを削除します。

- **隔離: ファイルからウイルスを駆除して元の場所に戻す**: 感染ファイルからウイルスを駆除し、駆除済みのファイルをクライアントの元の場所に戻します。なお、ウイルスが駆除できなかったファイルは、引き続き、隔離領域に保管されます。
- **隔離: 元の場所に戻す**: ファイルを隔離領域からクライアントに戻します。※隔離されたファイルを元の場所に戻すと、ファイルは感染した状態のままコンピュータ上に存在し続けます。
- **隔離: G Data セキュリティラボに送信**: 未知ウイルスの検出もしくはその疑いがある場合は、隔離機能を使ってファイルをG Data まで送付してください。分析解析後、新種ウイルスの場合は、ワクチン更新で対応ワクチンを提供いたします。送付されたデータは、個人情報保護の方針に則り、G Data セキュリティラボにて慎重に取り扱います。
- **レポートを削除**: 選択した対象レポートを削除します。※隔離領域にあるファイルに関するレポートを削除するには、2度確認を求められます。レポートを削除すると、隔離領域にあるファイルも一緒に削除されます。
- **関連レポートを削除**: 複数の異なるジョブやタスクを実行することで発生する、内容が重複するレポートやメッセージを削除します。

<u>ツールバーからの操作</u>

ツールバーでは、アイコン経由で簡単に操作ができます。以下のアイコンが利用できます。



更新: 表示を更新します。G Data マネジメントサーバー から最新レポートをロードします。



削除: 選択した対象レポートを削除します。隔離されているファイルに関連付けられたレポートを削除する場合は、確認が2回行われます。この後、隔離領域も一緒に削除されます。



印刷: レポートの印刷プロセスを開始します。画面が表示されるので、印刷するレポートの情報や領域などを選択します。



ページレイアウト: 印刷プレビューを表示します。



ウイルス駆除: 感染ファイルからウイルスを駆除します。駆除の結果は、一覧で表示されます。



隔離: 選択したファイルを隔離領域へ移動します。隔離領域に移動したファイルは、ウイルス本来の活動ができないよう、暗号化されてG Data マネジメントサーバー内の隔離領域に保存されます。オリジナルのファイルは削除されます。隔離領域内の各ファイルにはレポートが作成されます。※この隔離ファイルの関連レポートを削除すると、隔離領域内のファイルも一緒に削除されます。隔離領域のファイルは、ファイルの中身を分析させるため、G Data のインターネットレスキューに送付できます。送信するには、隔離レポート上で右クリックして、コンテキストメニューから選択します。



ファイルを削除: クライアント上のオリジナルファイルを削除します。



ファイルを隔離領域から戻す: 隔離していたファイルを、隔離領域から元の場所（隔離前に保存されていたクライアント）に戻します。ファイルは、隔離時点の状態（感染したままの状態）で元の場所に戻されます。

 **ウイルスを駆除して、隔離領域から元の場所に移動**: ファイルからウイルスを駆除し、ウイルス駆除したファイルを隔離領域から元の場所（隔離前に保存されていたクライアント）に戻します。ウイルス駆除できない場合は、ファイルを隔離領域から元の場所（隔離前に保存されていたクライアント）に戻されません。

 **関連レポートを非表示**: 複数の異なるジョブやタスクを実行することで発生する、内容が重複するレポートやメッセージを非表示にして、最新のレポートだけが表示されるようになります。

 **既読レポートを非表示**

 **すべてのレポートを表示**

 **エラーと情報に関するレポートのみ表示**

 **メールのレポートのみ表示**

 **駆除されなかったウイルスのレポートのみ表示**

 **隔離レポートのみ表示**

 **隔離領域の内容のみ表示**

 **HTTPレポートのみ表示**

 **バンクガードのレポートのみ表示**

 **ファイアウォールのレポートのみ表示** （G Data ClientSecurity Business / G Data EndpointProtection Business のみ）

 **ふるまい検知のレポートのみ表示**

 **アプリケーションコントロールのレポートのみ表示** （G Data EndpointProtection Business のみ）

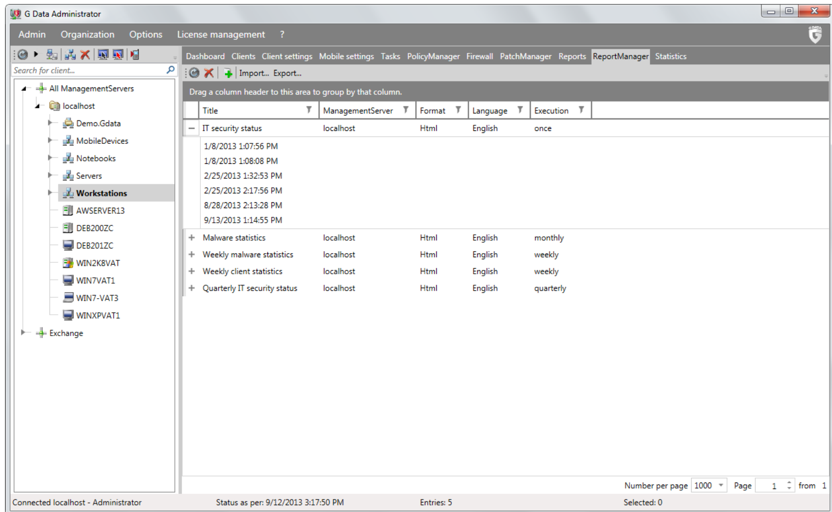
 **デバイスコントロールのレポートのみ表示** （G Data EndpointProtection Business のみ）

 **ウェブコンテンツコントロールのレポートのみ表示**（G Data EndpointProtection Business のみ）

 **MobileDeviceManagement のレポートのみ表示**

レポートマネージャー

レポートマネージャーでは、クライアントのステータスに関する情報を定期的に収集し、特定の受信者や受信グループに配布する事ができます。



 **更新**: 表示を更新します。

 **削除**: 選択したアイテムを削除します。

 **新規レポートスケジュールを追加**: 新規レポートを定義し、レポートジョブをスケジューリングします。

エクスポート/インポート: **レポートの定義**をバックアップするには、［**エクスポート**］をクリックして「.dbdat」ファイル形式で保存してください。定義を復元するには、［**インポート**］をクリックしてください。

作成済みの定義を選択後に右クリックすると、**削除**、**今すぐ実行**などの操作を実行できます。**プロパティ**からは定義の編集をすることができます。また、実行済みの定義では、レポートジョブが実行済みの場合は、**履歴**からレポート実行日時を確認したり、結果を表示させたりすることができます。

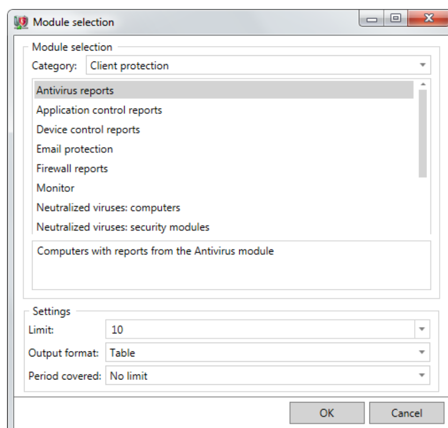
レポートの定義

レポートの定義では情報収集用のレポートモジュールを自由に設定する事ができ、レポートマネージャーは、そのモジュールに基づいてクライアントから必要な情報を指定した間隔で収集します。

新規レポートスケジュールを追加のアイコンを押して表示されるウィンドウでは、レポートに**名前**を付けたり、レポートの**言語**を設定したりできます。また、**送信先グループ**では、レポートを受け取る受信者を設定できます。ここでは、**オプション** > **サーバー設定** > **メール設定**で作成したグループ、もしくは直接新しいグループを作成して設定に適用することができます。また、**追加の送信先**では、追加のメールアドレスを追加できます。なお、複数入力する場合は、コンマ（,）で区切る必要があります。

1回のみのレポート（**実行**で**1回**にチェックを入れた場合）を行う場合は、開始時間を選択します。定期的に実行するレポートでは、実行頻度を選択（**毎日**、**毎週**、**毎月**、**3ヶ月毎**、**半年毎**、**毎年**から選択可）してから、実行日時を設定してください。

毎日にチェックを入れると、曜日を選択できるようになり、この設定で2日ごとのレポートや特定曜日のみのレポートが可能になります。



レポートにモジュールを追加するには、左下の［**新規**］を押して、**モジュール選択画面**を開いてください。レポートモジュールは、**クライアント: 一般** と **クライアント: 保護** の2つのカテゴリに分類されています。カテゴリを選択後、表示されるモジュールから適当なものを選択してください。**設定**では、様々な出力形式（**表**、**折れ線グラフ**、**棒グラフ**、**円グラフ**）を選択できます。出力形式はモジュールによって利用できるものと利用できないものがあります。

特定モジュールでは、**制限**や**対象期間**などの設定することで、表示データを制限したり、特定期間のデータのみを表示させることができます。選択したモジュールをレポートに追加するには、［OK］をクリックしてください。

編集、**削除**ボタンを使用すると、設定したモジュールの編集や削除を行えます。モジュールの選択と設定の完了後に、［**プレビュー**］を押すと、設定した内容のレポート例が表示されます。

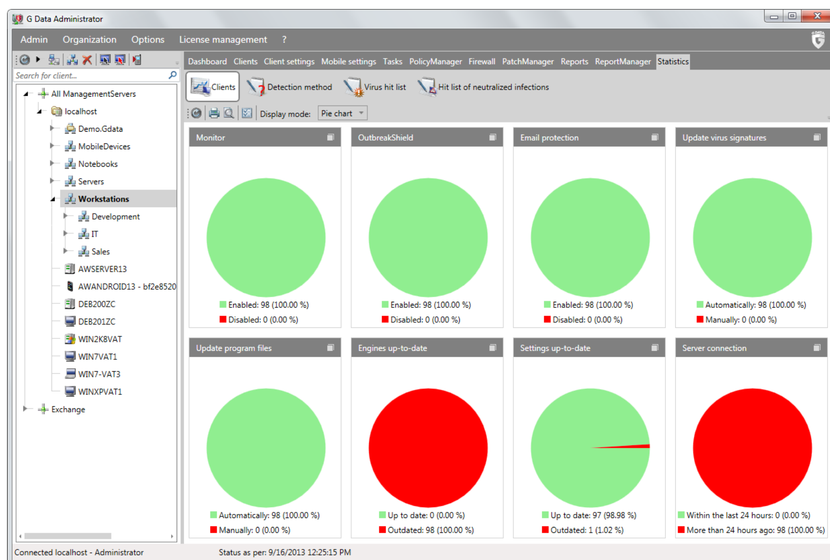
レポートジョブを実行すると、作成されたレポートは**レポートマネージャー**で閲覧できるようになり、送信先にもレポートが送付されます。レポートの内容を確認するには、各レポートの左端にある[+]アイコンをクリックし履歴を開いた後、表示したいレポートの日付をダブルクリックしてください。

レポート履歴の確認やレポートプレビューを行う場合は G Data Administrator を使用しているPC上に Internet Explorer 8 以上がインストールされている必要があります。

統計

統計では、ネットワーク内のウイルス感染や防御状況などのステータスをチェックすることができます。画面上部のボタンから表示させたいカテゴリを選択してください（**クライアント**、**検出方法**、**検出したウイルス**、および**保護したクライアント**から選択可）。

表示モードではテキストやグラフでの表示（棒グラフ、円グラフなど）を選ぶことができます。



G Data WebAdministrator

G Data WebAdministrator は、ウェブベースで動作する G Data ManagementServer の制御モジュールです。インターネットに接続できれば、ウェブブラウザを使用して、通常の G Data ManagementServer と同じ感覚で遠隔地から管理作業を行うことができます。

G Data WebAdministrator の起動方法

インストールの完了後、G Data WebAdministrator を任意のブラウザから起動することができます。インストール後にデスクトップに作成されたアイコンをダブルクリックするか、インストールプロセスの最後に表示されたURLを直接入力してアクセスしてください。アクセス用のURLは、**IIS と WebAdministrator がインストールされているPC**のIPアドレスまたはコンピュータ名、およびフォルダ名で構成されています (例 *http://10.0.2.150/GDAdmin/*)

※ 主にWinsows 8 において、ログイン画面が表示され、各種情報を正確に入力しているにも関わらず、サーバーにログインできない場合は .NET Framework 4.5 の機能有効化が不十分な場合があります。
Windowsの機能の有効化または無効化画面から、.NET Framework 4.5 の階層を開き、WCFサービス 以下の HTTPアクティブ化、TCPアクティブ化、TCPポート共有にチェックが入っているかを確認してください。

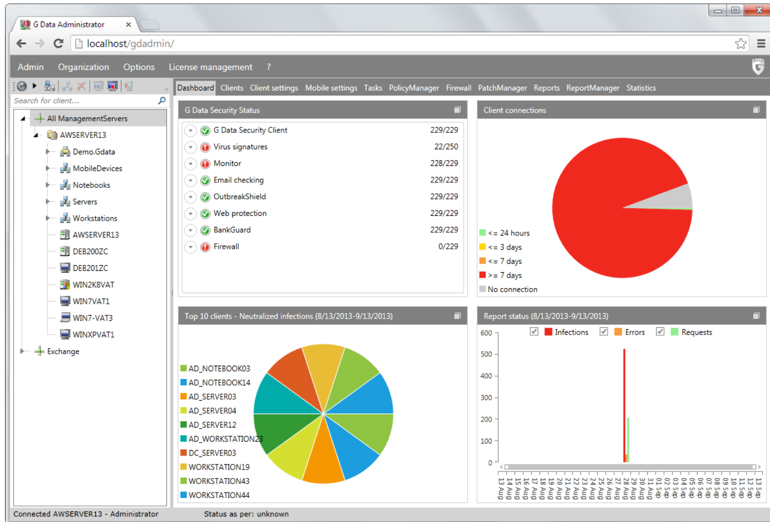
※ G Data WebAdministrator をインストール、使用するためには、Windowsの機能からIIS（インターネットインフォメーションサービス）を有効化しておく必要があります。

※ G Data WebAdministrator の起動には、ブラウザプラグインに Microsoft Silverlight が必要です。インストールされていない場合は、あらかじめダウンロードとインストールを行ってください。

G Data WebAdministrator のログイン画面は、通常の G Data Administrator と同じログイン方法をサポートしています。ログインする際は、**言語、サーバー名（もしくはIPアドレス）、認証、ユーザー名とパスワード** を入力、設定します。
認証の選択部分では、Windowsの資格情報を使用してログインする場合は、**Windows認証**を選択。G Data Administrator で設定したアカウントを使用してログインする場合は、**統合認証**を選択してください。
それぞれの項目の入力や設定が完了したら、**OK**ボタンを押してログインを行います。

G Data WebAdministrator の使用方法

G Data WebAdministrator のインターフェイスは、G Data Administrator とほぼ同じ内容です。初回のログイン後には、ダッシュボードが表示され、G Data ManagementServer に登録された各クライアントの管理状況を確認する事ができます。



G Data WebAdministrator の各機能は、G Data Administrator と同様です。機能の詳細は G Data Administrator 内の各項をご参照ください。

※G Data WebAdministrator では一部のOSにおいてIMEを使用した日本語入力ができない場合があります。その際に日本語を入力をする必要がある場合は、テキストエディタなどで必要な日本語を入力し、コピーした後、 G Data WebAdministrator の入力欄にテキストを貼り付けてください。

G Data MobileAdministrator

G Data MobileAdministrator は、スマートフォンなどのモバイル端末から G Data ManagementServer を操作できる管理画面です。この画面はモバイル端末での操作に最適化されており、管理作業において使用頻度の高い設定を簡単に確認、変更する事ができます。

G Data MobileAdministrator の起動方法

インストールの完了後、G Data MobileAdministrator を任意のブラウザから起動することができます。ブラウザを起動し、インストールプロセスの最後に表示されたURLにアクセスしてください。アクセス用のURLは、**IIS と WebAdministrator がインストールされているPC**のIPアドレスまたはコンピュータ名、およびフォルダ名で構成されています (例 *http://10.0.2.150/GDMobileAdmin/*)

※ 主にWinsows 8 において、ログイン画面が表示され、各種情報を正確に入力しているにも関わらず、サーバーにログインできない場合は .NET Framework 4.5 の機能有効化が不十分な場合があります。
Windowsの機能の有効化または無効化画面から、.NET Framework 4.5 の階層を開き、WCFサービス 以下の HTTPアクティブ化、TCPアクティブ化、TCPポート共有にチェックが入っているかを確認してください。

※ G Data MobileAdministrator をインストール、使用するためには、Windowsの機能からIIS（インターネットインフォメーションサービス）を有効化しておく必要があります。

MobileAdministrator のログイン画面は G Data Administrator と WebAdministrator と同じログイン方法をサポートしています。ログインする際は、**サーバー名（もしくはIPアドレス）**、**認証**、**ユーザー名とパスワード**、**言語** を入力、設定します。
認証の選択部分では、ドメインの資格情報を使用してログインする場合は、**Windows認証**を選択。G Data Administrator で設定したアカウントを使用してログインする場合は、**統合認証**を選択してください。
次回以降の情報入力の手間を省きたい場合は**ユーザーデータを記録**を選択します。**言語**では管理画面の表示画面を指定できます。それぞれの項目の入力や設定が完了したら、**ログイン**ボタンを押してログインを行ってください。

G Data MobileAdministrator の使用方法

G Data MobileAdministrator にログインすると、メインメニューが表示されます。

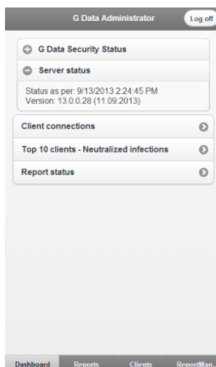
ここでは以下の項目を利用できます:

・**ダッシュボード**
・**レポート**
・**クライアント**
・**レポートマネージャー**

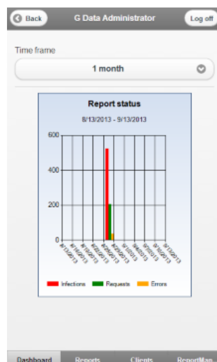
ログオフを行う場合は、画面右上の **ログオフ** ボタンをタップしてください。

ダッシュボード

G Data MobileAdministrator のダッシュボード画面では、最も重要な統計を一目で確認する事がすることができます。 G Data Administrator のダッシュボードのように、G Data ManagementServer とそのクライアントのステータスの概要の表示、クライアント接続と保護状況についての統計を表示することも可能です。



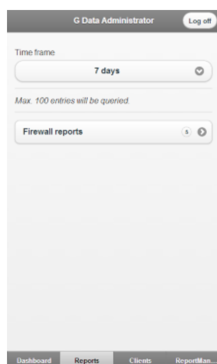
サーバおよびクライアントのステータスに関する全体的な情報を表示するには、**G Data セキュリティステータス** を選択します。G Data Security Client のインストール状況、ワクチン（定義ファイル）が古くなっていないか、ウイルスガード、メールチェック、アウトブレイクシールド、ファイアウォール、といった各種機能の動作状況、これらの情報が一覧できます。また、**ワクチン**をタップして内容を表示すると、**ワクチンのロールバック**を管理することができます。
G Data ManagementServer自体の状態は、**サーバーステータス**を開くことで表示できます。



クライアント接続、保護したクライアントトップ10 、**レポートステータス**、をそれぞれタップする事で、感染状況やエラーの統計を確認する事ができます。

レポート

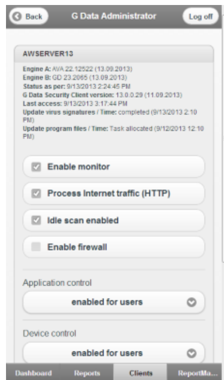
レポート画面では、ウイルス、ファイアウォール、ポリシーマネージャーのレポートを表示できます。表示される内容は、G Data Administrator の**レポート**画面で確認できる情報と同じ内容が、モバイル端末用に最適化されたものです。
※使用している製品により、表示できる情報は異なります。



レポートを表示する際は**期間**を 1日、7日、1ヶ月 から選択します。期間を選択すると、さまざまなカテゴリのレポートが一覧されますので、表示したいカテゴリをタップし、内容を確認してください。その際、名前によってフィルタをかけることもできます。それぞれのレポート内容は更にタップする事で、対応用の操作を行うことも可能です。

クライアント

クライアント画面では G Data ManagementServer によって管理されているクライアントの概要を一覧する事ができます。クライアントごとの詳細確認を行う事ができ、いくつかのセキュリティ設定を変更する事も可能です。



クライアント画面では、まず初めに G Data ManagementServer によって管理されているすべてのマシンのリストが表示されます。このリストは名前でフィルタリング可能です。

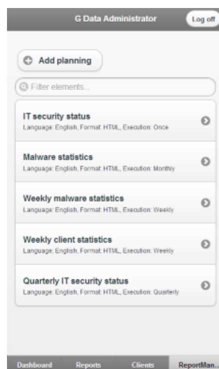
個々のマシンを選択することで、ワクチンのバージョンなど、いくつかの統計情報を確認できます。ここでは、いくつかのセキュリティ設定を編集することも可能です。
ウイルスガード、**インターネットコンテンツのスキャン**、**アイドリングスキャン**、**ファイアウォール**など、各種機能名のチェックボックスを操作する事で、機能を有効または無効化できます。※使用している製品により、設定できる項目は異なります。

EndpointProtection を使用している場合は、**アプリケーションコントロール**、**デバイスコントロール**、**ウェブコンテンツコントロール**、**インターネット利用時間**などのポリシー設定を、この画面で制御することができます。

最後に、**保存** をタップする事で、変更を加えた設定を保存できます。

レポートマネージャー

レポートマネージャー画面では、G Data Administrator の **レポートマネージャー** 画面同様に、レポートジョブを作成、編集、スケジュール化したり、プレビューする事ができます。



新しいレポートジョブを追加するには、**プランニングを追加**をタップします。既存のジョブはレポートマネージャーのメイン画面に表示され、それらをタップして編集することができます。

ジョブ画面では、ジョブの内容をを編集することができます。そこで、ジョブの**名前**、**言語**、**送信先グループ**、**追加の送信先**（複数可）を設定してください。
ジョブの**間隔**を選択し、**実行時間**や**実行日**を定義することによってレポートをスケジュール化することができます。

選択したモジュールでは、レポートに含めるモジュールを選択することができます。（これらは、G Data Administrator で使用できるモジュールと同じものです。）
モジュールを追加、編集もしくは、削除した後に、**保存**をタップすると、モジュールの設定が保存され、ジョブ画面に戻ります。

設定が完了した後は、必要に応じてレポートをプレビューし、それを**保存**します。**削除**をタップする事で不要なジョブを削除することも可能です。

G Data Security Client

G Data Security Client は、G Data ManagementServer からのジョブをクライアントPCのバックグラウンドで実行しながら、クライアントをウイルスから保護するモジュールです。クライアントには、それぞれのワクチンとスキャンジョブを自由に操作できる権限を付与することも可能です。これにより、クライアントがネットワーク外で利用する環境下（G Data ManagementServer に接続できない状態）でも、必要に応じて、クライアント側でウイルススキャンの指示を実行できます。

トレイアイコン



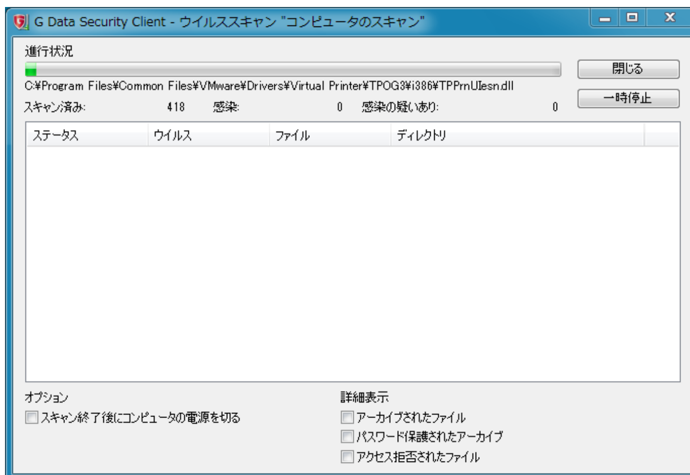
G Data Security Client のインストール後は、クライアントPCのタスクバーにアイコンが表示されるようになります。

このアイコン上で右クリックすると、G Data Security Client のコンテキストメニューが開き、ここから許可されている操作が実行できます。

ユーザーが操作できるオプションは、G Data Administrator の**クライアント設定**機能で管理します。

ウイルススキャン

G Data Administrator で指定したスキャン実行時刻以外に、クライアントPCのユーザーがウイルススキャンを手動実行することができます。



スキャン対象には、**リムーバブルメディア**、**CD/DVD-ROM**、**メモリとスタートアップ**、**特定のファイル/ディレクトリ** を指定できます。ローカルユーザーに対してこの機能を利用できる権利を付与すると、会社のネットワークに定期的に接続されていないノートPC ユーザーでのウイルス感染や感染拡大を回避できる可能性があります。なお、検出されたウイルスはローカルの隔離フォルダに移動されます。

特定のファイルもしくはディレクトリをスキャンするには、対象の上で右クリックし、表示されたコンテキストメニューから **ウイルススキャン**を選択します。

ウイルススキャン進行状況のステータスウィンドウは、ウイルススキャンがローカルで開始された場合にのみ表示されます。

ウイルススキャン中は、コンテキストメニューに以下の項目が拡張表示されます:

- **スキャン優先度**: ウイルススキャンの優先度を設定できます。スキャン優先度を**高**に設定すると、本製品によるウイルススキャンをコンピュータ上で実行されている他のプログラムより優先して処理します。これにより、スキャンの所要時間が短くなりますが、コンピュータ上の別のプログラムの処理速度は遅くなります。一方、**低**に設定すると、スキャンの所要時間は長くなりますが、他のプログラムの処理速度にはあまり影響が出ません。（ウイルススキャンがローカルで開始された場合のみ利用できます）

- **ウイルススキャンを停止**: ローカルのクライアントPC上で実行されているウイルススキャンを一時停止します。※

- **ウイルススキャンをキャンセル**: ローカルのクライアントPC上で実行されているスキャンをキャンセルします。※

  ※この機能は、以下の設定において利用できます。

  G Data Administrator > クライアント設定 > ユーザーによるウイルススキャンの実行を許可 が有効に設定されているクライアント環境において、クライアントユーザー自身がスキャンを開始した場合

  G Data Administrator で設定できるスキャンジョブの**プロパティ**で、**ジョブの停止またはキャンセルを可能にする**（ジョブのタブ）が有効に設定されている場合

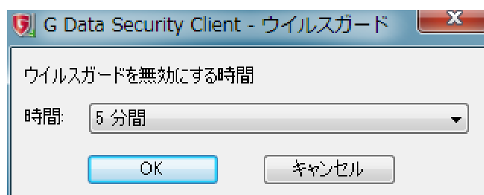
- **スキャンウインドウを表示**: 実行中のウイルススキャンのステータスウインドウを表示します。（ウイルススキャンがローカルで開始された場合のみ利用できます）

ウイルスガードを無効にする

クライアントPC上で稼動中のウイルスガード機能を一定期間だけ（**5 分 〜 コンピュータを次回再起動するまで**） 無効にできます。例えば、大量のファイルをコピーする際に、ウイルスガードによるチェックを省いてコピー速度を向上させたい場合などは、ウイルスガードを無効にすると効果的です。

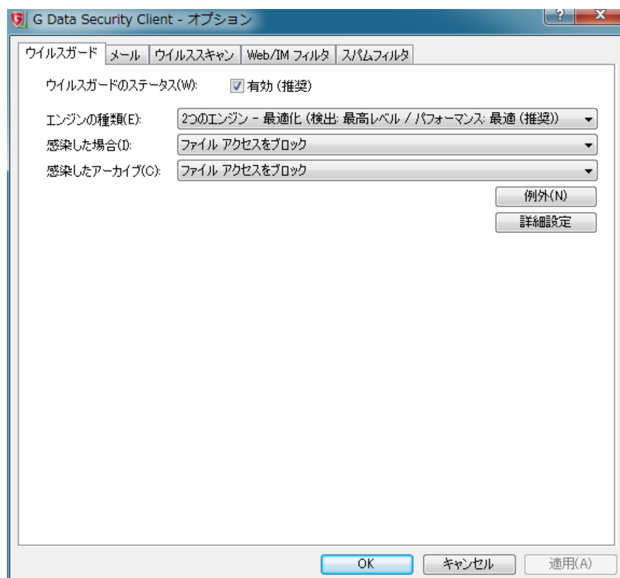
※この機能は、**G Data Administrator > クライアント設定**で管理者からこの権利を割り当てられている場合にのみ可能です。

※ウイルスガードを無効にするとリアルタイム監視が無効になり、保護能力が大きく低下しますので、必要な場合にのみ実行するようにしてください。



オプション

管理者によって、**ユーザーによるウイルスガード/メールオプションの変更を許可**が有効にされている場合は、クライアントユーザーは使用しているコンピュータのスキャンやウイルスガードやメールスキャンなどの設定を必要に応じて変更できます。特に、ウイルスガードのオプションを変更できる権限を付与した場合、クライアント上のウイルス保護機能をすべて無効化できるため、専門知識があるユーザーだけが操作できるように制限してください。各設定についての詳細は**クライアント設定**内の項目でご確認いただけます。



クライアントで操作できる**オプション**のセキュリティ関連の設定については、各クライアントPCに対してパスワードで保護できます。この場合、管理者が個々のクライアントにそれぞれパスワードを付与し、ユーザーはそのパスワードを使ってクライアントのウイルス保護機能を変更します。このパスワードは、G Data Administrator > クライアント設定 > **オプション変更をパスワードで保護** を有効にした後、 **パスワードを変更**から設定できます。

隔離

G Data Security Client がインストールされたクライアントには、隔離領域がローカルに作成されます。隔離領域に移動したファイルは、暗号化され、実行不可能な状態になって保管されます。この時、1MB以上のファイルはローカルの隔離領域に保存され、1MB未満の隔離ファイルは、G Data ManagementServer の隔離領域にへ移動されます。（これは大量のファイルによるネットワーク負荷を抑えるための動作で、この設定は変更できません）

G Data ManagementServer に接続されていない環境、例えばノートPC上などでウイルス（サイズ: 1MB未満）が検出された場合、このウイルスはローカルの隔離領域に保存され、G Data ManagementServer との次回接続時に、マネジメントサーバー側の隔離領域に移されます。

隔離領域では、ファイルに感染したウイルスを駆除して正常な状態に戻す、それが不可能な場合はそのファイル自体を削除する事ができます。必要であれば、隔離領域から元の保存場所に隔離されたファイルを戻すことも可能です。

注意: 隔離領域に移動しただけでは、ウイルスは駆除されません。ウイルスが駆除されていないファイルを隔離領域から元の場所へ移動する際は、くれぐれも注意してください。このオプションは、感染ファイルなしにはプログラムが動作しない場合で、そのファイルがデータ復旧に必要な場合にのみ選択してください。

隔離領域の保存場所: 隔離領域はそれぞれ以下の場所に保存されています。

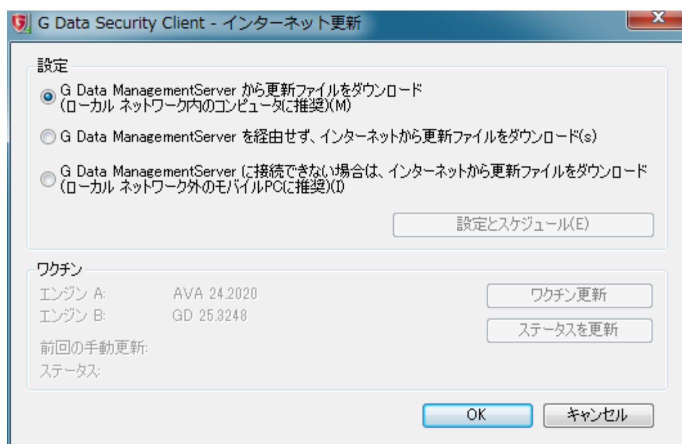
クライアント側
Windows XP: Documents and Settings\All Users\G DATA\AntiVirusKit Client\Quarantine
それ以降のOS: ProgramData\All Users\G DATA\AntiVirusKit Client\Quarantine

マネジメントサーバー側
Windows XP: Documents and Settings\All Users\G DATA\AntiVirus ManagementServer\Quarantine
それ以降のOS: ProgramData\G DATA\AntiVirus ManagementServer\Quarantine

インターネット更新

G Data Security Client はワクチン更新の際、G Data ManagementServer を経由せずにインターネットから直接ロードすることもできます。この設定は、G Data Administrator によって、クライアントごとに有効化することができます。

設定とスケジュールからは、クライアントにおけるワクチン更新のスケジュール設定が可能です。



ファイアウォール

クライアントのファイアウォールに関する様々な設定が可能です。

この設定を操作できるようにするには、**G Data Administrator > ファイアウォール > ユーザーによるオフサイトコンフィグレーションの変更を許可** を有効にする必要があります。

詳細は、G Data Administrator の**ファイアウォール**の項を参照してください。

※ファイアウォール機能は、G Data ClientSecurity / G Data EndpointProtection に搭載されています。

ファイアウォールを無効/有効にする

クライアント側でファイアウォールを無効化/有効化する事ができます。

この機能を操作できるようにするには、**G Data Administrator > ファイアウォール > ユーザーによるファイアウォールの有効/無効を許可** を有効にする必要があります。

情報

インストールされているプログラムおよびワクチンに関する情報（バージョンおよび提供日時）を表示します。

G Data Internet Security for Android

本製品をご利用いただいているお客様は、Android 端末の管理に利用できる、ビジネスバージョンの G Data Internet Security for Android をご利用いただけます。この G Data Internet Security for Android は G Data Administrator 経由で端末にインストール可能です。

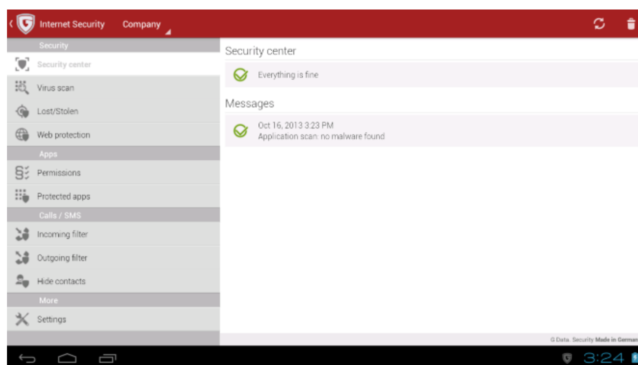
セキュリティ

画面左上の G Data アイコンをタップする事で表示されるこのメニューには、G Data Internet Security for Android の機能が一覧されます。ここに表示される機能は G Data Administrator の **モバイル設定** で管理する事ができます。また、権限が付与されている場合は、端末自身でもいくつかの設定を行う事が可能です。

セキュリティセンター

アプリ起動時に最初に表示されるセキュリティセンター画面では G Data Internet Security for Android の主なセキュリティ機能の動作状況が表示されます。マルウェアに感染している場合やワクチンが古くなっている場合などには**セキュリティセンター**領域に警告が表示され、**メッセージ**領域には、その警告や処理の履歴、スキャン結果やワクチン更新の概要などが表示されます。

スキャンのログは、スキャン結果のメッセージをタップする事で詳細を確認する事ができ、それ以外のメッセージもタップする事でメッセージに応じた操作を行う事ができます。（スキャンのログはアプリの **設定 > 一般** で有効/無効を設定する事ができます）

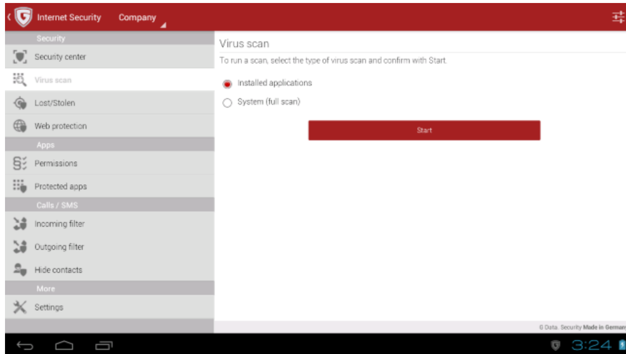


画面右上にある、円状の矢印の形をしたアイコンをタップするとワクチンの更新を行う事ができ、ゴミ箱のアイコンをタップするとメッセージ領域のメッセージをすべて削除する事ができます。

スキャン

この画面ではマルウェアのスキャンを手動で行う事ができます。スキャンを行う際は次の方式を選択できます:

- **インストール済みアプリ**: このスキャン方式では、端末にインストールされているアプリを対象としてマルウェアをスキャンします。マルウェアが端末上で検出された場合は、G Data Internet Security for Android の画面経由で削除する事ができます。
- **システム (完全スキャン)**: このスキャン方式では、端末のストレージ全体を対象としてマルウェアをスキャンします。マルウェアの早期発見に役立ち、例えば、インストールされる前にSDカード上の悪意のあるアプリを検出、削除することが可能です。



定期的なスキャンを設定するには、画面右上にある **設定アイコン** や **セキュリティ>設定** から表示できる **定期スキャン** オプションで設定できます。これらの設定は、G Data Administrator の **モバイル設定** を介してリモート管理することもできます。

盗難/紛失対策

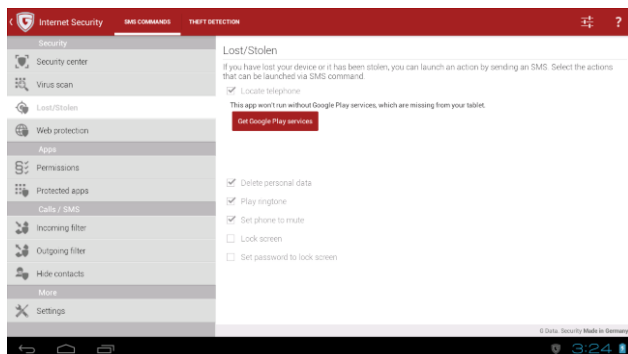
この機能は、盗難されたり、紛失したモバイル端末を保護するために使用できます。

SMS コマンドは、この機能が有効になった端末にSMS経由でコマンドを送信する事で、盗難や紛失に対する様々な対策を行うことができる機能です。**盗難検出機能**では、盗難された端末のSIMカードが入れ替えられた際の対策を行う事ができます。

初めてこの機能を使用する際は、この機能に使用する、**パスワード**、**電話番号**、**メールアドレス**の入力を求められます。G Data Administrator の **モバイル設定 > 盗難対策** であらかじめ設定しておくか、アプリ上の**盗難/紛失対策**の画面から入力してください。アプリ画面上の右上の設定アイコンから、これらの情報を後から設定し直すことも可能です。

SMS コマンド

この機能が有効になった端末に対して SMS コマンドを利用する事で、盗難や紛失に対する様々な対策を行うことができます。



機能を有効にした後は、SMSコマンドで実行できる対策を自由に設定する事ができます。使用したい機能にチェックを入れて有効化してください。

※リモート管理を許可している場合、この機能は G Data Administrator の **モバイル設定 > 盗難対策** で設定します。

設定が完了した後は、盗難/紛失機能が有効化された端末にSMSでコマンドを送ることで各機能を実行できます。その際は、先に設定したSMSコマンド用のパスワードを含めて送信する必要があります。

SMSコマンド一覧:

以下は、端末にSMSで送信できるコマンド一覧です。コマンドへの回答は通常、SMSコマンドの送信元デバイスに送信されます。メールアドレスでの返答が行われるコマンドは、機能に登録したメールアドレスに結果が送信されます。

※ コマンド（太字）とパスワード（斜体）の間には半角スペースを入力する必要があります。
※ コマンド内の半角スペースや記号も間違いなく入力する必要があります。

入力例
1234をパスワードとし、位置情報送信のコマンドを送る場合
1234 locate　(文字で記載すると　1234半角スペースlocate　となります)

- **端末の位置を特定**: 機能に登録したメールアドレスに、コマンドを受けた端末の位置情報が送信されます。（GPSの情報が利用されます）
  SMSコマンド:　*SMSコマンド用パスワード* locate

- **データを消去**: 端末を工場出荷時の状態にリセットします。すべてのデータは削除されます。
  SMSコマンド:　*SMSコマンド用パスワード* wipe

- **着信音を鳴らす**: シグナル音を再生します。例えば、近くにある端末を探す場合に役立ちます。
  SMSコマンド:　*SMSコマンド用パスワード* ring

- **ミュートに設定**: 紛失した端末の場所をを音で特定されたくない場合などに、ミュートに設定できます。この場合でも、コマンドによるシグナル音の再生は可能です。
  SMSコマンド:　*SMSコマンド用パスワード* mute

- **画面をロック**: 画面をロックします。画面ロック用のパスワードが設定されていない場合は、SMSコマンド用のパスワードが適用されます。
  SMSコマンド:　*SMSコマンド用パスワード* lock

- **画面ロック用のパスワードを設定**: 画面ロック用のパスワードを設定します。このコマンドの送信後、画面をロックコマンドを送信し、画面をロックしてください。
  SMSコマンド:　*SMSコマンド用パスワード* set device password: *画面ロックに使用するパスワード*

- **パスワードのリセット**: SMSコマンド用のパスワードを新たに設定します。このコマンドは機能に登録した電話番号から送信する必要があります。
  SMSコマンド:　remote password reset: *新しいSMSコマンド用パスワード*

盗難検出機能

端末が盗難され、新たなSIMカードが挿入された場合は、端末にSMSコマンドを送信できなくなります。その状況に備えてSIMカードが交換された時の対策を選択できます。

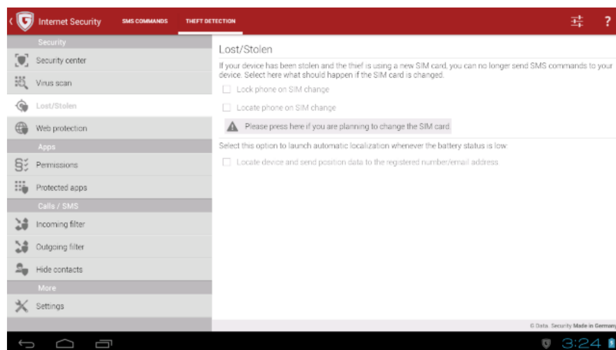
※リモート管理を許可している場合、この機能は G Data Administrator の **モバイル設定 > 盗難対策** で設定します。

盗難検出機能一覧:

- **SIM交換時にデバイスをロック**: SIMカードが交換もしくは取り除かれた際に、端末が自動的にロックされます。オリジナルのSIMカードが再び挿入されるとロックは解除されます。

- **SIM交換時にデバイスの場所を特定**: SIMカードが交換もしくは取り除かれた際に、端末の現在位置を自動的にメール送信します。このメールは機能に登録していたメールアドレス宛に送信されます。

自分でSIMカードを交換する場合は、**SIMカードを交換する場合は、ここをタップしてください。**と表示された領域をタップします。
その後、端末の電源を切り、新しいSIMカードに交換した後再起動を行うと、新しいSIMカードが盗難防止機能に登録されます。

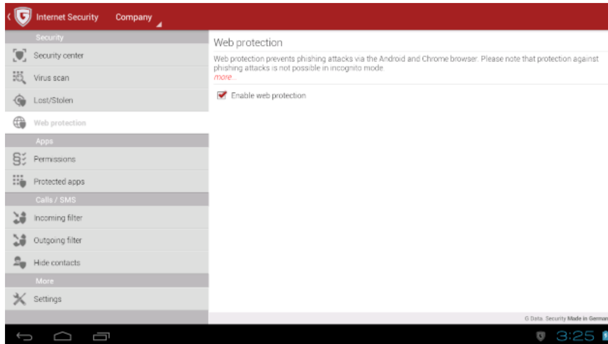


バッテリー残量が少なくなった際、GPS情報をもとにして端末の位置を自動的に特定したい場合は、**端末の位置を特定し、設定した電話番号/メールアドレスに位置情報を送信** を有効にしてください。
盗難/紛失対策機能に登録しているメールアドレス宛に、省電力モードに移行する前に最後に端末のあった場所が送信されるようになります。

ウェブ保護

ウェブ保護機能はフィッシング詐欺や悪質サイトの攻撃から Android のデフォルトブラウザと Chrome を保護します。
※シークレットモード（シークレットブラウジング）では、保護は適用されません。
ウェブ保護がフィッシングサイト、悪質サイトのリストに照合する作業には、通常よりも通信が必要となります。アプリ内メニューの **設定** > **ウェブ保護** の領域で、**Wi-Fi接続時に限定**を有効にすることで意図しない通信量の増加を防ぐことができます。

この設定は G Data Administrator の **モバイル設定** > **一般** でも設定可能です。



アプリ

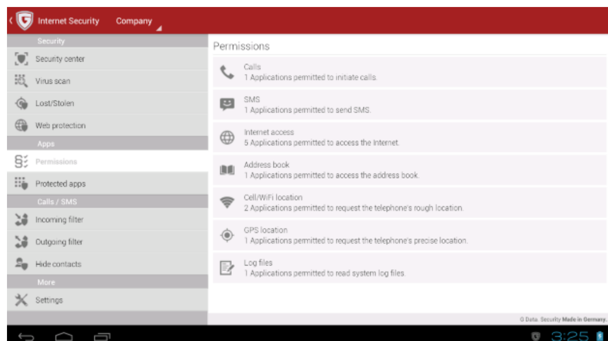
アプリの領域には、インストールされたアプリの権限の監視や、アプリの利用をブロックするための機能が用意されています。

権限の監視

この機能では、インストールされているアプリに割り当てられている権限を一覧する事ができます。

どのアプリが各権限を利用しているかを調べるには、それぞれの権限名（**電話**、**SMS**、**連絡先**など）をタップしてください。選択した権限を利用しているアプリが一覧され、不信と思われるアプリは直接アンインストールする事ができます。また、必要に応じてアプリを**アプリ保護**に追加する事も可能です。

※リモート管理を許可している場合は、アンインストールのみ可能です。



アプリ保護

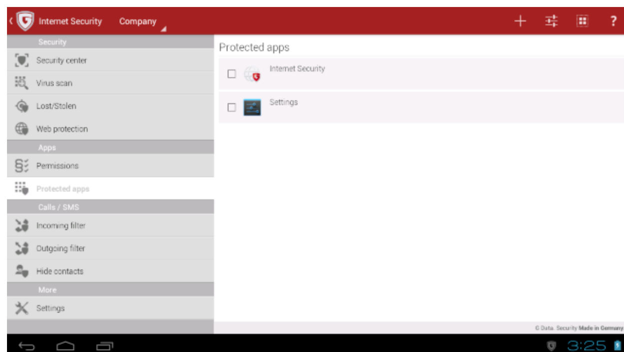
アプリ保護機能を使用すると、端末上の特定アプリにパスワードをかけて利用をブロックする事ができます。例えば Play ストアにブロックをかけて、勝手にアプリなどを購入される事を防ぐといった事に活用できます。

※リモート管理を許可している場合、この機能は G Data Administrator の **モバイル設定 > アプリ** で設定します。

アプリ上で初めてこの機能を使用する際は、**パスワード**、**メールアドレス**、**セキュリティ保護用の質問**の入力を求められます。

パスワードには、ブロックしたアプリを起動する際に入力するパスワードを設定します。
メールアドレス、**セキュリティ保護用の質問**には、設定したパスワードを忘れた際にパスワードを確認するためのアドレスもしくは質問を設定します。

各項目を入力し終わった後は、設定を保存するために画面左上の**フロッピーディスクのアイコン**をタップしてください。



アプリ保護のメイン画面には、この機能で保護されているアプリが一覧されます。保護するアプリを追加するには、画面右上にある + ボタンをタップしてください。

アプリの追加画面では、**推奨**、**ダウンロード**、**すべて** からアプリの一覧方法を選択できます。一覧されたアプリの中から保護したいアプリにチェックを入れ、画面左上のチェックマークをタップ、もしくは端末の**Backボタン**でアプリ保護のメイン画面に戻ると保護が開始されます。ここで保護されたアプリを起動する際は、アプリ保護で設定したパスワードの入力を求められます。

アプリ保護を解除するには、メイン画面の保護されたアプリの一覧から解除したいアプリにチェックを入れ、画面左上のチェックマークをタップ、もしくは端末の**Backボタン**を押すと、解除が適用されます。

電話 / SMS

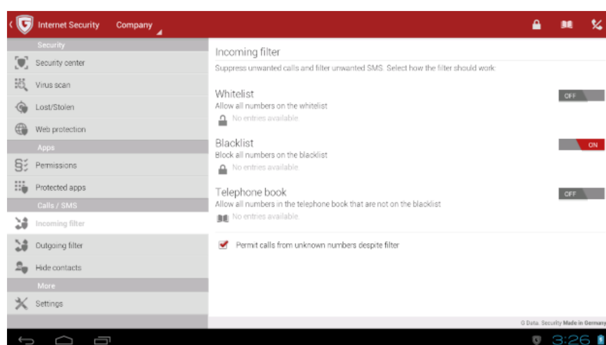
電話 / SMSの領域には、発着信のフィルタリングや、連絡先表示の制御をおこなう機能が用意されています。

着信用フィルタ

この機能で電話やSMSの着信をフィルタできます。フィルタには、許可された電話番号からの着信を許可する**ホワイトリスト**、許可しない電話番号からの着信をブロックする**ブラックリスト**の2つの種類があります。**連絡先**は端末の電話帳に登録されている電話番号からの着信を許可するオプションで、ホワイトリスト、ブラックリストと併用する事ができます。

非通知番号からの着信を許可するには、**フィルタを無視して、非通知番号からの着信を許可**にチェックを入れてください。

※リモート管理を許可している場合、この機能は G Data Administrator の **モバイル設定 > 通話フィルタ** で設定します。



着信用フィルタ画面の右上にある、**電話帳のアイコン**から端末に登録されている連絡先の一覧の確認、**受話器のアイコン**から着信拒否した電話/SMSの履歴を確認できます。

ホワイト、ブラックリストを有効化している場合は、電話/SMSフィルタのメイン画面右上にある**鍵のアイコン**をタップすると、リストの編集画面に移動します。編集画面の右上にある + ボタンをタップすると、連絡先もしくは電話履歴から連絡先を一覧できます。そこからリストへ登録したい連絡先にチェックを入れ、画面左上のチェックマークをタップ、もしくは端末の**Backボタン**を押すと、指定した連絡先がリストへ登録されます。

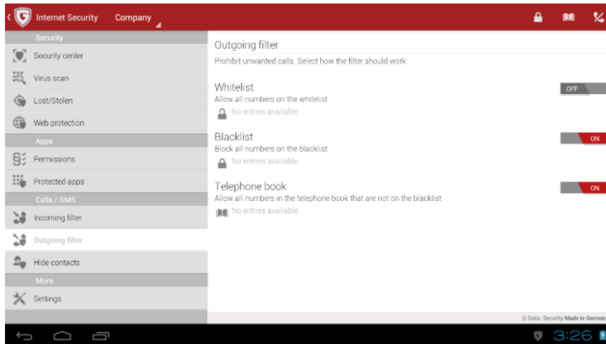
※電話番号の選択画面で、再度右上の + アイコンをタップする事で、新規の電話番号を登録する事もできます。

※新規の番号を登録する際は、電話番号の後にアスタリスク（*）を入力する事で、特定の番号で始まる電話番号をすべて含めることができます。
例: 050で始まる電話番号をすべて含めたい場合は 050* と入力します

発信用フィルタ

この機能で電話やSMSの発信をフィルタできます。フィルタには、許可された電話番号からの着信を許可する**ホワイトリスト**、許可しない電話番号からの着信をブロックする**ブラックリスト**の2つの種類があり、**着信用フィルタ** と同じ方法で設定できます。

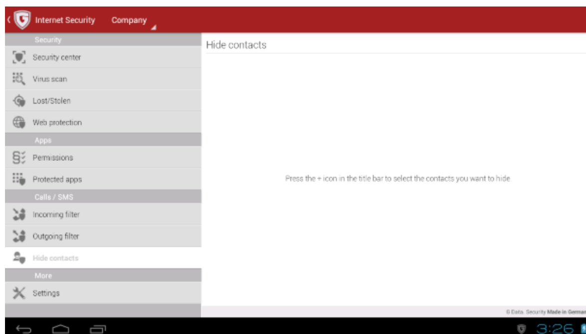
※リモート管理を許可している場合、この機能は G Data Administrator の **モバイル設定 > 通話フィルタ** で設定します。



連絡先の非表示

この機能を使用すると、指定した連絡先の着信履歴と電話帳内の連絡先を非表示にする事ができます。この機能に登録された連絡先は電話帳内の G Data 用アカウントに移動され、着信などのアクセスがブロックされます。

※リモート管理を許可している場合、この機能は G Data Administrator の **モバイル設定 > 連絡帳** で設定します。



連絡先を隠す機能のメイン画面には、機能が有効になっている連絡先が一覧されます。
機能に連絡先を登録する場合は、画面右上にある + ボタンをタップし、連絡先もしくは電話履歴の中から連絡先を選択してください。

登録を行った後は、メイン画面に表示されているそれぞれの連絡先をタップする事で、非表示のオプションの選択画面に移動できます。

着信を非表示では、着信とSMSを非表示にするかどうかを設定、**連絡先を非表示**では、端末の電話帳から連絡先を非表示にするかどうかを設定します。同画面にある**メッセージ履歴**、**電話履歴**、では非表示にした着信など確認できます。

連絡先を隠す機能から登録してある連絡先を削除したい場合は、その連絡先をタップし続けて、**項目を削除**を選択してください。すると一覧から連絡先が削除され、端末の電話帳に連絡先が戻ります。

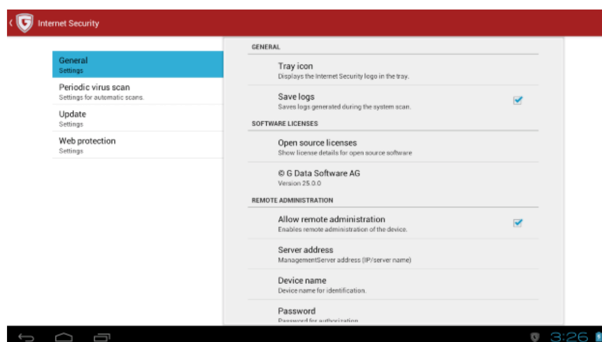
※連絡先を非表示/ON の状態で G Data Internet Security for Android を削除した場合、非表示の連絡先が削除されます。 必ず、 G Data Internet Security for Android の削除前に、連絡先を非表示/OFF の状態にする、もしくは連絡の非表示機能からすべての連絡先の登録を削除して下さい。

設定

G Data Internet Security for Android は G Data Administrator の **モバイル設定** で設定を変更する事ができます。アプリ画面左上のG Dataアイコンをタップする事で表示されるメニュー内の**設定**からも、いくつかの設定を変更する事が可能です。

一般

この領域では、OSのステータスバーのロゴ表示と、スキャンログに関する設定を行う事ができます。



- **通知アイコン**: G Data Internet Security for Android のアイコンをステータスバーに表示するかどうかを設定できます。

- **ログを保存**: スキャンのログを保存するかどうか設定できます。

リモート管理の領域では、リモート管理を行うにあたってのサーバー設定を行う事ができます。

- **リモート管理を許可する**: G Data ManagementServer による管理を行うためには、この設定を有効にする必要があります。
- **サーバーアドレス**: G Data ManagementServer のサーバー名もしくは、IPアドレスを入力します。
- **端末名**: 管理する際に識別しやすいよう、端末に名前を設定できます。
- **パスワード**: G Data ManagementServer との認証に使用するパスワードを入力します。 このパスワードは G Data Administrator のオプションメニュー内にある **サーバー設定** > Mobile 画面の**モバイルクライアント用認証**で設定します。

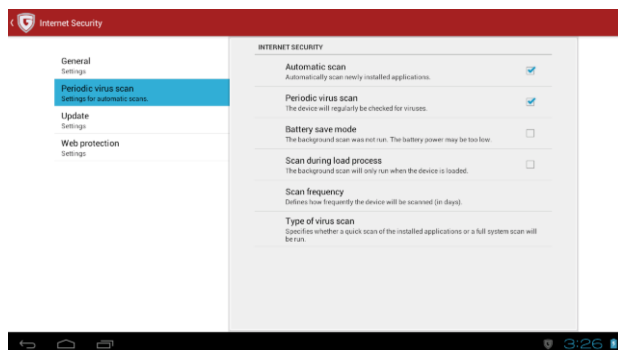
定期スキャン

この領域では、定期スキャンに関する設定を行う事ができます。

設定できる項目：

- **自動スキャン**: 新しくインストールされたアプリを自動的にスキャンします。
- **定期スキャン**: 定期的にスキャンを自動で実行します。
- **省エネモード**: バッテリーの残量が残りわずかな場合、バックグラウンドスキャンを実行しません。
- **充電時にスキャン**: デバイスが充電中の場合のみ、バックグラウンドスキャンを実行します。
- **スキャン頻度**: 定期スキャンを実行する頻度を設定します。 (1, 3, 7, 14, 30 日ごとから選択できます).
- **スキャンの種類**: 定期スキャンで実行するスキャンの種類を設定します。

上記の設定は G Data Administrator の **モバイル設定** > **一般** でも設定できます。



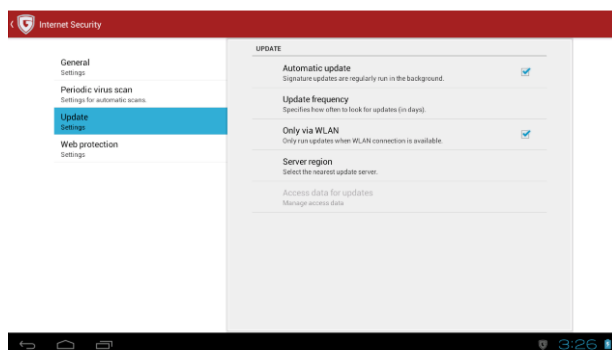
自動更新

この領域では、ワクチン更新や更新サーバに関する設定を行う事ができます。

設定できる項目：

- **自動更新**: 定期的にワクチン更新をバックグラウンドで実行します。
- **更新頻度**: 更新を検索する頻度を設定します。 (1, 3, 7, 14, 30 日ごとから選択できます)
- **Wi-Fi接続時に限定**: Wi-Fi経由での接続時にのみ、更新を実行します。
- **更新サーバー**: 更新用の接続先サーバーを選択します。 デフォルト設定では、最初の更新を行った際に一番近い地域のサーバーが自動的に選択されるようになっています。

更新サーバー以外の設定は G Data Administrator の **モバイル設定** > **一般** でも設定できます。



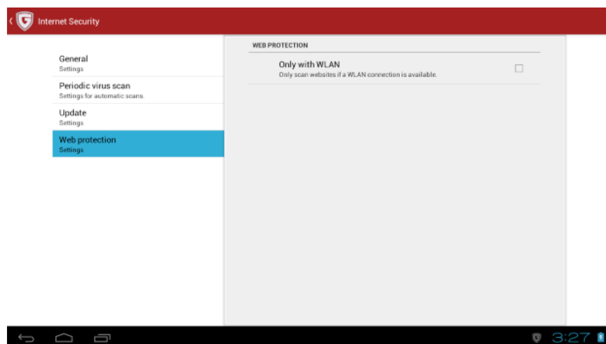
ウェブ保護

この領域では、ウェブ保護の動作制限に関する設定を行う事ができます。

設定できる項目：

- **Wi-Fi接続時に限定**: Wi-Fi経由での接続時にのみ、ウェブサイトをチェックします。

上記の設定は G Data Administrator の **モバイル設定** > **一般** でも設定できます。



トラブルシューティング（FAQ）

インストール

Q. G Data Security Client のインストール後に、一部のアプリケーションの動作速度が遅くなった場合の対処

通常、ウイルスガードによるリアルタイムスキャンで、システム動作に大幅に支障をきたすケースはほとんどありませんが、1つのアプリケーションで同時に沢山のファイルを開いたり、一部のファイルを繰り返し開くと、システムの動作速度が落ちる場合があります。

この問題を回避するには、ウイルスガードを一時的に無効にして、この問題がウイルスガードに起因するものであるかを確認します。サーバー上のファイルにアクセスする場合は、このサーバーのウイルスガードも一時的に無効にする必要があります。

動作速度低下がウイルスガードに起因する場合

アクセス頻度の高いファイルに対し、例外設定を行います。アクセス頻度が高いファイルを特定するには、G Data が提供するツール **MonActivity** を使用して、例外設定するファイルを特定します。**MonActivity** は、以下のG Data 法人向けサイト（英語）からダウンロードしてください。

MonActivityダウンロード先URL

https://www.gdatasoftware.co.uk/downloads.html

上記URLでToolsを選択しMonActivityCSをダウンロードしてください。

> ウイルススキャンを1 種類のエンジンだけで稼動させると、パフォーマンスを大幅に向上させることができます。詳しくは G Data Aministrator の **クライアント設定 / ウイルスガード** の項を参照してください。

動作速度低下がウイルスガードに起因していない場合

G Data Security Client がインストールされているPCに、以前他社製セキュリティがインストールされていた場合は、そのデータの残骸と本製品の機能がぶつかり合っている可能性があります。その状況を解消するには、G Data Security Client をアンインストールし、**AVCleaner** で完全アンインストールした後、以前インストールされていたセキュリティソフトの完全アンインストールツールを使用し、完全アンインストール、その後 G Data Security Client を再インストールしてください。なお、他社製品の完全アンインストールツールに関しては、使用していたセキュリティソフトのユーザーサポートにお問い合わせください。

AVCleanerダウンロード先URL

https://www.gdatasoftware.co.uk/downloads.html

上記URLでToolsを選択しAVCleanerをダウンロードしてください。

Q.
ユーザー認証せずにインストールした場合で、後からユーザー認証する方法

インストール時の**製品登録**の画面で、**後で認証を行う**を選択し、認証をまだ実行していない場合は、以下の手順で認証を実行します。

認証方法

1. **スタート > すべてのプログラム > G Data > G Data ManagementServer > インターネット更新** を開きます。
※WIndows8の場合はスタート画面から、インターネット更新を開きます。

2. **G Data マネジメントサーバー - インターネット更新**の画面の中にある **[オンライン登録]** ボタンをクリックします。

3. **更新サーバーにログイン**の画面が表示されるので、必要事項と一緒に、**レジストレーション番号**を入力します。

4. 正常に登録が行われるとアクセスデータ（ユーザー名とパスワード）がポップアップで表示されます。ここで表示されるアクセスデータは、忘れないようにメモしてください。メモが終わったら登録完了です。

- ユーザー認証を行うには、インターネット接続が必要です。

- レジストレーション番号が認証されない場合は、番号が正しく入力されているかどうかを確認してください。 使用しているフォントの種類によっては、大文字の「i」（India の i）を、数字の「1」や小文字の「l」（London の l）と読み違えることがよくあります。他にも「B」と「8」、 「G」と「6」、 「Z」と「2」といった間違えもあります。

- アクセスデータは必ず書き留めて、厳重に保管してください。ポップアップ表示されたアクセスデータは、ウィンドウ内のチェックボックスにチェックを入れ、[OK] をクリックするまで消えません。

- 入力したレジストレーション番号で認証できない場合は、まず入力ミスの可能性がないか確認してください。更に問題が解決できない場合は、ユーザーサポートまでお問い合わせください。

- **後で認証を行う** を選択して製品をインストールした場合は、G Data AntiVirus Business としてインストールされます。G Data ClientSecurity Business / G Data EndpointProtection Business に含まれる **ファイアウォール** や **ポリシーマネージャー** の機能は、認証後に有効化され、利用できるようになります。

エラーメッセージ

Q. クライアント側で
「プログラムファイルが変更された、または破損しています。」と表示された場合の対処

クライアントプログラム自体にエラーが発生すると、**「プログラムファイルが変更された、または破損しています」**というメッセージが G Data Administrator のレポート画面に表示されます。

このメッセージが表示された場合

1. まずメッセージを閉じ、G Data の更新サーバーから最新のプログラムファイルをダウンロードします。

2. 次に、問題が発生したクライアントでプログラムファイルを更新します。

上記の方法で解決しない場合は、クライアントの再インストールをお試しください。

Q.
クライアント上で「ワクチンが破損しています。」と表示された場合の対処

「ワクチンが破損しています。」というメッセージは、ワクチンのデータベースにエラーが発生した場合に G Data Administrator のレポート画面に表示されます。

このメッセージが表示された場合

1. まずメッセージを閉じ、G Data Managementserverで最新のワクチンをダウンロードします。

2. 次に、問題が発生したクライアントで、ワクチンを更新します。

上記の方法で解決しない場合は、クライアントの再インストールをお試しください。

Linux版の使用方法

Q. Linux file server が G Data ManagementServer へ接続できず、ワクチン更新できない場合の対処

1 以下の G Data Security Client の両プロセスが稼動しているか、確認してください。

ターミナルに以下のコマンドを入力します。

linux:~# ps ax|grep av

以下の結果が出力されます。

... Ssl 0:07 /usr/sbin/avkserver --daemon

... Ssl 0:05 /usr/sbin/avclient --daemon

これらのコマンドは、どのLinuxディストリビューションでも共通のコマンドです。

スタート:

linux:~# /etc/init.d/avkserver start

linux:~# /etc/init.d/avclient start

ストップ:

linux:~# /etc/init.d/avkserver stop

linux:~# /etc/init.d/avclient stop

注意: この操作を実行するには、Linuxコンピュータに管理者 (=“root“) 権限でログインしている必要があります。

2 ログファイルの内容を確認するには、**/var/log/** に収納されているログファイル（**gdata_install.log**）を参照してください。このファイルには、リモートインストールプロセスのログが保存されています。

/var/log/gdata のディレクトリには、**avkclient.log** が保存されています。このファイルには、**avkserver**（スキャナ）のスキャン結果と **avclient** プロセス（G Data ManagementServer と接続するプロセス）のアウトプットが収められています。

上記のファイルでエラーメッセージを探します。さらにメッセージを参照する場合は、コンフィグレーションファイル **/etc/gdata/gdav.ini** および **etc/gdata/avclient.cfg** で、**LogLevel** のエントリに **7** を入力してください。

注意: ログレベルの設定が高すぎると、多量のメッセージが生成され、ログファイルは増大します。ログレベルは低い数値に設定してください。

3 スキャナをテストします。

avkclient （コマンドラインツール）を使用して、以下のコマンドを実行し、**avkclient** （スキャンサーバー）の機能をテストしてください。

linux:~$ **avkclient avkversion** - ワクチンのバージョンと更新日をアウトプット

linux:~$ **avkclient version** - バージョンを簡易形式でアウトプット

linux:~$ **avkclient scan:<file>** - <file> をスキャンし、結果をアウトプット

4 コンフィグレーションファイルを確認します。

etc/gdata/avclient.cfg に **avclient** （リモートクライアント）のコンフィグレーションファイルがあります。メインの ManagementServer（MainMMS）のアドレスが正しく入力されていることを確かめてください。

入力されたアドレスが正しくない場合は、エントリを消して G Data ManagementServer のアドレスを入力してください。

5 共有設定をテストしてください。

Samba共有ディレクトリのウイルス保護は、**/etc/samba/smb.conf** （Sambaコンフィグレーションファイル）に以下のエントリを入力し、有効にします。

vfs objects = gdvfs

[global] のセクションにエントリがある場合は、すべての共有ディレクトリに保護が有効となっています。他のセクションにラインが表示されると、その共有ディレクトリに対してのみ保護が有効になっています。

ウイルス保護なしでアクセスをテストするには、ハッシュキー (#) をプレフィックスに置いて、ラインをコメントアウトします。機能しない場合は、まずSambaのコンフィグレーションに問題がないか、確認してください。

6 Linux Workstation ウイルスガード

avguard （ウイルスガードプロセス）が稼動しているか、確認してください。

linux:~# ps ax|grep avguard

ウイルスガードには、redirfs と avflt （カーネルモジュール）が必要です。lsmod| grep redirfs と lsmod| grep avflt.のモジュールがロードされているか、lsmod で確認してください。

モジュールは使用するカーネルによってコンパイルされているはずです。

この処理は Dynamic Kernel Module System (DKMS) が行います。DKMSは適合するカーネルヘッダパッケージと共に、ディストリビューションにインストールされています。DKMSがインストールされている場合は、自動的にDKMSがモジュールをコンパイルし、インストールします。

ウイルスガードのログデータは、/var/log/gdata/avguard.log で確認できます。

その他

Q. クライアントとマネジメントサーバーの接続状況の確認方法

クライアントタブの**最終アクセス日時**には、クライアントが最後に G Data マネジメントサーバーと通信した時間が表示されます。G Data ManagementServer のデフォルト設定では、5 分間隔で通信を行い、動作状況や設定の同期を行います。（スキャンジョブが動作していない場合）

クライアントとマネジメントサーバーの接続ミスが発生する場合は、まずは以下の点を確認してください。

- **クライアントPCの電源がオフの状態、もしくはネットワークと未接続**

  →クライアントの電源を入れる、もしくはネットワークへ接続してください。

- **クライアントとマネジメントサーバー間で TCP/IP 接続が未確立**

  →ネットワーク設定を確認してください。

- **名前解決が正常に機能していないため、クライアントがサーバーのIPアドレス取得に失敗**

  サーバー側はポート7161、**クライアント側**はポート7167が開かれている必要があります。コマンドプロンプトで Telnet コマンドを使い、接続状況を確認します。

  コマンド記述方法: telnet <SERVERNAME> <PORTNUMBER>

  Windows Vista、Windows 7、Windows 8 、Windows Server 2008 (R2)、Windows Server 2012 またはそれ以降のOSでは、デフォルト状態ではTelnetコマンドが利用できないため、当該機能を有効にする必要があります。

クライアントからサーバーへの接続に問題がない場合は、コマンドプロンプト上に意味をなさない確認用の文字列が表示されます。また、サーバーからクライアントへの接続に問題がない場合は、空の入力ウィンドウが現れます。

Q. 隔離領域に移されたメールボックスを元の場所に戻す方法

メールボックスに感染したメールがある場合、メールボックス全体が隔離される可能性があります。その際は以下の方法で、ファイルを元の場所へ移動してください。

メールボックスを元の場所へ戻す方法

1 メールボックスが隔離されたクライアントのメールプログラムを終了します。

※この際、メールボックスのあるディレクトリに新しいアーカイブファイルが作成されている場合は、それを削除してください。

2 G Data Administrator を起動します。

3 G Data Administrator 上で、メールボックス隔離の関連レポートを開き、[**ファイルを元の場所に戻す**] をクリックします。

Q.
コンピュータ名ではなく、IPアドレスを使って、クライアントPCと通信する方法

G Data ManagementServer とクライアントPC間の通信を**コンピュータ名**ではなく、**IPアドレス**で行うには、以下の方法で設定します。

G Data ManagementServer を使用するPCでの設定

G Data Manatement Serverをインストール後、以下のレジストリ内のデータをIPアドレスに書き換えます。

32bit OS の場合
HKEY_LOCAL_MACHINE\SOFTWARE\G DATA\AVK ManagementServer\ComputerName

64bit OS の場合
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\G DATA\AVK ManagementServer\ComputerName

G Data SecurityClient を使用するPCでの設定

- G Data SecurityClient をリモートインストールする場合

  G Data ManagementServer で上記のIPアドレス設定を行った後、リモートインストールを行うと自動的に G Data ManagementServer に認識されます。
  先にインストールしてあった G Data Security Client が、G Data ManagementServer に認識されない場合は、クライアントPC上で以下のレジストリ内のデータを G Data ManagementServer のIPアドレスに書き換えます。

  32bit OS の場合
  HKEY_LOCAL_MACHINE\SOFTWARE\G DATA\AVKClient\Server

  64bit OS の場合
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\G DATA\AVKClient\Server

- G Data SecurityClient を製品メディアでインストールする場合

  G Data SecurityClient を 製品メディアからインストールする際、通常はサーバー名とコンピュータ名の入力が求められますが、これらの入力欄に適切な IP アドレスを入力します。

Q. ワクチンファイル、隔離領域、G Data ManagementServer のデータベースなどの保存場所

G Data Security Client 上のワクチンファイル

- Windows XP/Server 2003/Server 2003 R2: C:\Program Files\Common Files\G DATA\AVKScanP\BD or G Data

- Windows Vista/Windows 7/Windows 8/Server 2008/Server 2008 R2/Server 2012: C:\Program Files (x86)\Common Files\G DATA\AVKScanP\BD or G Data

G Data ManagementServer 上のワクチンファイル

- Windows XP/Server 2003/Server 2003 R2: C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Updates

- Windows Vista/Windows 7/Windows 8/Server 2008/Server 2008 R2/Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Updates

G Data Security Client 上の隔離領域

- Windows XP/Server 2003/Server 2003 R2: C:\Program Files\Common Files\G DATA\AVKScanP\QBase

- Windows Vista/Windows 7/Windows 8/Server 2008/Server 2008 R2/Server 2012: C:\Program Files (x86)\Common Files\G DATA\AVKScanP\QBase

G Data ManagementServer 上の隔離領域

- Windows XP/Server 2003/Server 2003 R2: C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Quarantine

- Windows Vista/Windows 7/Windows 8/Server 2008/Server 2008 R2/Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Quarantine

G Data ManagementServer データベース

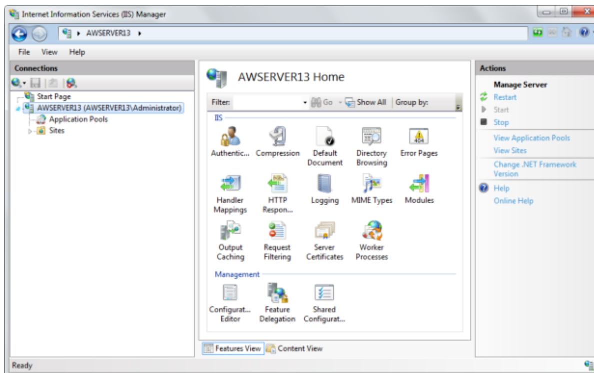
Windows XP/Windows Vista/Windows 7/Windows 8/Server 2003/Server 2003 R2/Server 2008/Server 2008 R2/Server 2012:

- C:\Program Files\Microsoft SQL Server\MSSQL.1 \MSSQL\Data\GDATA_AntiVirus_ManagementServer.mdf
- C:\Program Files\Microsoft SQL Server\MSSQL.1 \MSSQL\Data\GDATA_AntiVirus_ManagementServer_log.ldf

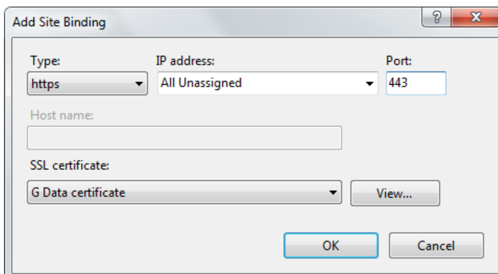
Q. IIS 7 / 7.5 / 8 でSSLサーバ証明書を有効化する方法

クライアントと WebAdministrator/ MobileAdministrator 間の通信を暗号化して安全に行うためには、インターネットインフォメーションサービス（IIS）でSSLサーバ証明書を有効にすることをお勧めします。

SSLサーバ証明書を有効化するには、IIS 7 、7.5 (Windows Vista, Windows 7, Windows Server 2008/R2)、8 (Windows 8, Windows Server 2012)の **インターネットインフォメーションサービス (IIS) マネージャー** を使用します。 Windows Server 2008 の場合、IIS マネージャーは **スタート** > **すべてのプログラム** > **管理ツール** から開く事ができます。他の方法では **スタート** > **ファイル名を指定して実行** にコマンド *inetmgr* を入力して実行してください。このコマンドは Windows 7 / 8 でも有効です。（Windows 8 の場合は検索画面にこのコマンドを入力してください。）



証明書を作成するには、IISマネージャーの画面左にある **通信** パネルでサーバーを選択し、画面中央の IIS カテゴリー内にある **サーバー証明書** をダブルクリックします。画面が切り替わったら、画面右の **操作** パネルにある **自己署名入り証明書の作成** をクリックします。次に表示されたダイアログで、証明書のフレンドリ名を入力してOKをクリックすれば、証明書が作成され、サーバー証明書パネルに表示されます。
※ 証明書の有効期限は、デフォルト設定の場合作成日から1年後に設定されますのでご注意ください。



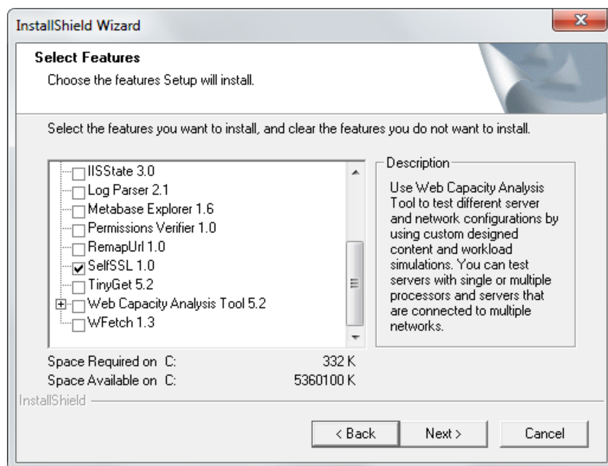
証明書をサイトの通信に利用するには、まず画面左の **接続** パネルから適切なサイトを選択し、画面右の **操作** パネルから **バインド** を選択してください。次に、表示されたダイアログで **追加** をクリックしサイトバインドを追加します。この時、**種類** には https を選択し、**SSL 証明書** には先ほど追加した証明書を設定してください。 **OK** をクリックすればバインドの設定が完了します。

これらの設定が完了した後、実際に WebAdministrator / MobileAdministrator を暗号化通信を介して安全に利用するには、アクセス用のアドレスの *http://* を *https://* に置き換えてアクセスしてください。例 *https://servername/gdadmin*.

※ ここで説明した方法で自己署名による証明書をサーバに設定した場合、WebAdministrator / MobileAdministrator にアクセスする際にブラウザが警告を発する場合があります。その場合でも問題は無く、通信が暗号化で保護された状態で安全にアクセスできます。

Q. IIS 5 / 6 でSSLサーバ証明書を有効化する方法

クライアントと WebAdministrator/ MobileAdministrator 間の通信を暗号化して安全に行うためには、インターネットインフォメーションサービス（IIS）でSSLサーバ証明書を有効にすることをお勧めします。



SSLサーバ証明書を有効化するには、IIS 5 (Windows XP) もしくは、IIS 6 (Windows Server 2003)の **SelfSSL** を使用します。SelfSSL は Microsoft のツールで、IIS 6.0 Resource Kit Tools に含まれます（Microsoft のウェブサイトから無料でダウンロード可能）。Resource Kit Tools のインストール時に **Custom** を選択し、**SelfSSL 1.0** を含めてインストール実行する事で、この機能が利用できるようになります。
インストール後に SelfSSL のコマンドプロンプトを開くには、**スタート** > **すべてのプログラム** > **IIS Resources** > **SelfSSL** > **SelfSSL** を実行してください。

証明書を作成するには、SelfSSL のコマンドプロンプトに以下のコマンドを入力し、**Enter** を押してください。

コマンド: *selfssl /N:CN=localhost /K:2048 /V:365 /S:1 /T*

次に作成の確認メッセージが表示されたら **Y** を押します。これによりローカルサーバ上のデフォルトIISサイトに証明書が作成され、localhost が信頼された証明書のリストに追加されます。ここで作成されたキーの長さは2048で、有効期間は365日になります。もし、サイトがIISのデフォルトサイトに設定されていない場合は、IISマネージャーでサイトの識別子を確認してください。その値に応じて、SelfSSL で入力する上記コマンドの */S:1* の値を変更してください。

※IISマネージャーは **スタート** > **すべてのプログラム** > **管理ツール** > **インターネットインフォメーションサービス (IIS) マネージャー** から開く事ができます。

これらの設定が完了した後、実際に WebAdministrator / MobileAdministrator を暗号化通信を介して安全に利用するには、アクセス用のアドレスの *http://* を *https://* に置き換えてアクセスしてください。例 *https://servername/gdadmin*.

※ ここで説明した方法で自己署名による証明書をサーバに設定した場合、WebAdministrator / MobileAdministrator にアクセスする際にブラウザが警告を発する場合があります。その場合でも問題は無く、通信が暗号化で保護された状態で安全にアクセスできます。

ウイルス被害に遭わないために

本製品には、業界最高水準の技術が搭載されており、既知ウイルスだけでなく、未知ウイルスに対して高い検出率を誇っています。最善の保護を実現するには、ウイルス対策ソフトのインストールの他に、コンピュータを使用するにあたって、日ごろからのユーザーの心がけも重要です。

ここでは、システムやデータの安全性を更に向上させる対策方法を紹介します。

- **複数のユーザーアカウントを使用する**: コンピュータにユーザーアカウントを 2 つ作ります。ひとつは**管理者アカウント**で、ソフトウェアをインストールしたりコンピュータの基幹的な設定を行う時にはこのアカウントを使用します。もうひとつは権限に制約のある**ユーザーアカウント**です。このユーザーアカウントでは、プログラムのインストールや Windows OS の変更をできないように権限を制限しておきます。このアカウントでログインすれば、比較的安全にインターネットや別のコンピュータからのデータ取得などを行うことができます。複数種類のユーザーアカウントを作成する方法は、Windows OS のヘルプを参照してください。

- **スパムメールを無視する**: チェーンメールやスパムメールに含まれているリンクや添付ファイルは、絶対開かないでください。また、これらのメールへの転送や返信もしないでください。

- **ウイルス感染の可能性がある場合は、すぐにスキャンする**: 新しくインストールしたソフトウェアが動作しない、またはエラーメッセージが表示されるなど、ウイルス感染が懸念される場合には、再起動する前に、問題のプログラムをスキャンしてください。再起動の前にスキャンする理由は、トロイの木馬は通常コンピュータの再起動時に削除コマンドを実行するので、再起動前にスキャンを実行する方がウイルスを検出、駆除できやすいためです。

- **定期的に Windows を更新する**: Microsoft から新たなパッチが提供されたら、速やかにダウンロードしてコンピュータにパッチをあてましょう。パッチを適用することで、Windows の脆弱性は修正され、攻撃者が脆弱性を利用した攻撃から防御できます。なお、Windows の更新は自動的に実行されるように設定しておきましょう。Windows XP などのパッチ配信が終了したOSの継続使用は非常に危険ですので、可能な限り早くサポート中のOSに切り替えてください。

- **オリジナルのソフトウェアを使用する**: ファイル共有サイトなどで出回っているソフトウェアは、ウイルス感染している可能性が非常に高いことが各種の分析や調査で実証されています。プログラムは必ずオリジナルのものを使用してください。出所の怪しいプログラムのダウンロードや利用は避けてください。

- **インターネットからダウンロードしたソフトウェアの取り扱いに注意する**: ソフトウェアをインターネットからダウンロードする際には、ダウンロード先のサイトの信頼性に十分に注意を払い、信頼できる供給元のソフトウェアだけを使用してください。また、心あたりのない送信者や、友人や同僚から予期せず届いたメールに含まれる添付ファイルは、決して開かないようにしましょう。ファイルを開く場合は、事前に送信者に確認をして、その安全性を確保してください。

使用許諾契約

G Data Software AG

ソフトウェア使用許諾契約書

G Data Software AG は、本使用許諾契約書のすべての条項に同意することを条件に、本ソフトウェアの使用許可をお客様に保証します。本使用許諾契約書に同意することによって、お客様と G Data Software AG の間に法的契約が締結されます。契約書の内容をよくお読みになってから、本製品をご利用ください。本契約書の条項に同意しない場合は、インストールを中断し本ソフトウェアをお使いにならないでください。

1. 契約の主題:

製造者 G Data Software AG は、お客様にソフトウェアを提供します。お客様には、本ソフトウェアを任意のコンピュータにインストールする譲渡不能の権利が付与されます。ただし、お客様がオリジナルのソフトウェアを所していることを条件として、本ソフトウェアを同時にインストールできるのは 1 台のコンピュータのみとします。ソフトウェアは、ランダム アクセス メモリ (RAM) にロードしたり、リードオンリー メモリ (ハードディスクやその他の保存媒体) にインストールしたりした時点で、コンピュータにインストールしたものと見なされます。お客様は、バックアップの目的で、購入したソフトウェアの複製を 1 部のみ作成することが許可されます。ただし、複製時には、既存の製品識別名、商標、著作権マークを更せずにそのまま継承するものとします。製品および付属文書を第者に譲渡することを禁じます。
ただし、事業全体を譲渡する場合、かつ本製品を事業資産の一部として第三者に開示する場合は、適用外とします。製造者はお客様の責任および費用負担を条件として、本製品を供給します。
本ソフトウェアのオンラインサービスでのご利用は、製造者の明示的な許可がある場合にのみ許可されます。

2. 支払い:

請求書のお受け取り後、請求書記の支払い期限内に請求金額の全額をお支払いいただくものとします。請求金額を全額お支払いいただくまでは、製品の所権は製造者によって留保されます。

3. 保証:

製造者は、本ソフトウェアがプログラム仕様書の記に従って使用可能であることを保証します。
現在の技術水準では、データ処理プログラムにすべての使用条件下でエラーがないことは保証できません。そのため、本プログラムに一切エラーがないことは保証いたしません。とりわけ製造者は、プログラムの機能がお客様の要件に適合することにつき、一切の保証を行いません。
本保証は、契約に基づく使用を前提とします。保証期間は、お客様へのソフトウェアの引渡し時点から開始します。製造者は、プログラム仕様書に基づいたソフトウェアの使用性に大きな影響がある場合に限り、ソフトウェアのエラーおよびプログラム仕様書からの逸脱を修正します。

4. 責任:

本ソフトウェアによって生じた結果損害に対しては、いかなる責任も負わないものとします。

5. その他の取り決め:

その他の取り決めおよび契約の更は、書面によってのみ効です。
万一、上記の条件のすべてまたは一部が無効とされた場合にも、本条件の残りの規定は依然として有効に存続します。本契約に関連して係争が生じた場合は、ドイツ、ボーフムの担当裁判所を裁判地とします。

重要

ソフトウェアをインストールすると、お客様は本使用許諾契約書のすべての条項に同意したものと見なされます。

Legal notices

SharpSerializer

Json.NET

DotNetZip

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

PhoneNumbers.dll / PushSharp

PhoneNumbers.dll and PushSharp are distributed under the Apache License 2.0 (www.apache.org/licenses).

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an

example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications,

or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

索引